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”
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

\[
\text{Break IO with prob } \varepsilon \implies \text{break FE with prob } \varepsilon/2^n
\]

Complexity leveraging inherent to IO? [GGSW’13]

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

\[
\text{Assumption}(C_0,C_1): \text{iO}(C_0) \approx \text{iO}(C_1)
\]

- 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

s.e. iO

GGHRSW'13

AJ'15,BV'15

poly iO

GGHRSW'13

poly FE

ts.e. FE

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
  ⇒ 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

$\begin{align*}
  m_0 &= 2 \\
  m_1 &= 1 \\
  m_3 &= 0 \\
  m_4 &= \_ \_ \\
\end{align*}$

Secret Key

$\begin{align*}
  f_0(x) &= x^2 - 3 \\
  f_3(x) &= 1 \\
  f_4(x) &= x + 1 \\
\end{align*}$

Decryption

$\begin{align*}
  f_0(m_0) &= 1 \\
  f_3(m_3) &= 1 \\
\end{align*}$
Slotted Functional Encryption

Private (slotted) encryption: encrypt in all slots

\[ m_0 \quad m_1 \quad m_3 \quad \perp \quad \perp \quad \perp \quad \perp \]

Ciphertext

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

Public (unslotted) encryption: encrypt in slot 0

\[ m \quad \text{pk} \]

Ciphertext

\[ m \]

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

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

\[
\begin{align*}
&f_0
\quad \downarrow
\quad \downarrow
\quad \downarrow
\quad f_3
\quad f_4
\end{align*}
\]

msk

\[
\begin{align*}
&f_0
\quad f_3
\quad f_4
\end{align*}
\]
Slotted Functional Encryption

**Unslotted keygen**: secret keys in slot 0

- Derived from slotted alg

```plaintext
f
msk
```

Secret Key
**Slotted Functional Encryption**

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

- $m_0$
- $f_0$
- $m_1$
- $f_3$
- $m_3$
- $f_4$

$f_0(m_0) = 1$

$f_3(m_3) = 1$

$f_0(m_0) = 1$

$f_3(m_3) = 0$

1

N/A
Slotted FE to (Unslotted) FE

Throw away slotted algorithms

\[
\operatorname{Enc}(\text{msk}, (m_0, m_1, m_2, \ldots ))
\]

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

\[
\operatorname{KeyGen}(\text{msk}, (f_0, f_1, f_2, \ldots ))
\]

\[
\operatorname{KeyGen}(\text{msk}, f)
\]

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

\[
\operatorname{KeyGen}(\text{msk}, f)
\]
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

- Slot Symm
- New Slot
- Strong Sk Moving

- Weak Ctxt Indist
- Strong Ctxt Indist

Lose 1 slot

= supported natively by our scheme
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

Ciphertext

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

Secret Keys

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

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

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

Dummy slot
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

Ciphertext

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

Secret Keys

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

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

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

Slot Duplication
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

<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>$f_3(x) = 1-x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f''_2(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

<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>$f_1(x) = 2-x^2$, $f'(x) = 2x+1$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_2(x) = 1-x$, $f''_2(x) = -x$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_3(x) = -x$</td>
</tr>
</tbody>
</table>

Weak Sk Moving
**Example Reduction: Strong Sk Moving**

**Goal:** move $f_1$ to third slot

<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>$f_2(x) = -1$</td>
</tr>
<tr>
<td>$m_4 = -1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
<tr>
<td></td>
<td>$f_4(x) = 2-x^2$</td>
</tr>
</tbody>
</table>

**Weak Sk Moving**
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

Ciphertext

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

Secret Keys

<table>
<thead>
<tr>
<th>$f_0(x)$</th>
<th>$f'_0(x)$</th>
<th>$f''_0(x)$</th>
</tr>
</thead>
<tbody>
<tr>
<td>$x^2$</td>
<td>$(-1)^x$</td>
<td>$1$</td>
</tr>
<tr>
<td>$2x+1$</td>
<td>$-1$</td>
<td>$(-1)^x$</td>
</tr>
<tr>
<td>$1-x$</td>
<td>$-1$</td>
<td>$(-1)^x$</td>
</tr>
<tr>
<td>$2-x^2$</td>
<td>$-1$</td>
<td>$(-1)^x$</td>
</tr>
</tbody>
</table>

Single Use Hiding
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

Ciphertext

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

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

Secret Keys

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

Single Use Hiding
### Example Reduction: Strong Sk Moving

**Goal:** move $f_1$ to third slot

<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>$m_4 = 1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
<tr>
<td></td>
<td>$f_3'(x) = 2x+1$</td>
</tr>
<tr>
<td></td>
<td>$f_3''(x) = -(-1)^x$</td>
</tr>
<tr>
<td></td>
<td>$f_4(x) = 2-x^2$</td>
</tr>
<tr>
<td></td>
<td>$f_4'(x) = -1$</td>
</tr>
<tr>
<td></td>
<td>$f_4''(x) = -(-1)^x$</td>
</tr>
</tbody>
</table>

**Weak Sk Moving**
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

<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>$f_2(x) = 2 - x^2$</td>
</tr>
<tr>
<td>$m_4 = 1$</td>
<td>$f_3(x) = 1 - x$</td>
</tr>
</tbody>
</table>
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

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

### Secret Keys

<table>
<thead>
<tr>
<th>Function</th>
<th>First Derivative</th>
<th>Second Derivative</th>
</tr>
</thead>
<tbody>
<tr>
<td>$f_0(x) = x^2$</td>
<td>$f'_0(x) = (-1)^x$</td>
<td>$f''_0(x) = 1$</td>
</tr>
<tr>
<td>$f_1(x)$</td>
<td>$f'_1(x) = 2x+1$</td>
<td>$f''_1(x)$</td>
</tr>
<tr>
<td>$f_2(x) = 2-x^2$</td>
<td>$f'_2(x) = -1$</td>
<td>$f''_2(x) = -(-1)^x$</td>
</tr>
<tr>
<td>$f_3(x) = 1-x$</td>
<td></td>
<td></td>
</tr>
</tbody>
</table>

Slot Duplication
### Example Reduction: Strong Sk Moving

**Goal:** move $f_1$ to third slot

<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>$f_2(x) = 2-x^2$</td>
</tr>
<tr>
<td>$m_2 = 1$</td>
<td>$f_3(x) = 1-x$</td>
</tr>
</tbody>
</table>

**Slot Duplication**
Example Reduction: Strong Sk Moving

Goal: move $f_1$ to third slot

<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></td>
<td>$f'_2(x) = -1$</td>
</tr>
<tr>
<td></td>
<td>$f_3(x) = 1-x$</td>
</tr>
</tbody>
</table>

$\begin{align*}
  m_0 &= 1 \\
  m_1 &= -1 \\
  m_2 &= 1 \\
  f_0(x) &= x^2 \\
  f'_0(x) &= (-1)^x \\
  f''_0(x) &= 1 \\
  f_1(x) &= 2x + 1 \\
  f'_1(x) &= 2x + 1 \\
  f''_1(x) &= -(-1)^x \\
  f_2(x) &= 2 - x^2 \\
  f'_2(x) &= -1 \\
  f''_2(x) &= -(-1)^x \\
  f_3(x) &= 1 - x
\end{align*}$
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]):

\[
\text{FE} \implies \text{Slotted FE} \implies \text{Cool stuff}
\]

Takeaway: slotted FE is useful abstraction in its own right
A New Crypto Landscape
A New Crypto Landscape

- **s.e. iO**
- **s.e. FE**
- **poly iO**
- **poly FE**
- **poly MMMaps**

**GGHRSW’13**

**AJ’15, BV’15**

**This work**

**All of Crypto**

- **FHE**

**Much of Crypto**

- **Traitor Tracing**
- **Witness PRFs/Enc**

**Some Crypto**

- **ORE**
- **PPAD Hardness** [GPS’15]
- **Multiparty NIKE** [GPSZ’16]
- **IBE**
- **ABE**
- **Deniable Enc**
- **Broadcast Enc**
- **TDP**
THANKS!