POLYNOMIAL TIME CRYPTANALYSIS OF THE SUBSPACE FLOODING ASSUMPTION FOR POST-QUANTUM iO

Aayush Jain (CMU), Huijia [Rachel] Lin (UW), Paul Lou (UCLA), Amit Sahai (UCLA)
INDISTINGUISHABILITY OBFUSCATION (iO)

\[ [BGI+01, GGH+13] \]

\[ C_0 \overset{iO}{\cong} C_0 \]

\[ C_1 \overset{iO}{\approx_{\text{comp}}} C_1 \]
OBFUSTOPIA

[SW13, GGH+13, BZ13, HKW15, BKW15, HJKSWZ16...]

(iO)

Short signatures
Perfect NIZKs for NP
CCA2-KEM
CCA2-Secure PKE
OT

Deniable Encryption
Universal Signature Aggregators
Functional Encryption
Non-interactive key agreement (NIKE)
Succinct Garbled RAM
OBFUstopia

i0 + Pseudorandom Oracle Model (PrOM) => Ideal Obfuscation [JLLW22]
OBFUSTOPIA

\[ iO + \text{Pseudorandom Oracle Model (PrOM)} \implies \text{Ideal Obfuscation} \] \cite{JLLW22}

can be heuristically instantiated by a hash function.
**OBFUSTOPIA**

\[i0 + \text{Pseudorandom Oracle Model (PrOM) } \Rightarrow \text{Ideal Obfuscation} \] [JLLW22]

Ideal obfuscation implies: Extractable witness encryption [GKPVZ13], Doubly Efficient PIR [BIPW17], OT from binary erasure channels [AIKNPPR21], Wiretap-channel coding [IKLS22] and more!!
Obfustopia

\[ iO + \text{Pseudorandom Oracle Model (PrOM)} \Rightarrow \text{Ideal Obfuscation} \ [JLLW22] \]

Ideal Obfuscation
OBFUSTOPIA

\( iO + \text{Pseudorandom Oracle Model (PrOM)} \Rightarrow \text{Ideal Obfuscation} \ [\text{[JLLW22]}] \)

Ideal Obfuscation

\( \mathcal{C}_0 \) : Chat-GPT23
- A personal assistant that knows your deepest and darkest secrets.
- Ideal obfuscated version can be captured and tortured, yet reveal nothing beyond input/output behavior.
CONSTRUCTING iO

Well-founded Assumptions

[JLS20, JLS21]

- LPN over $\mathbb{Z}_p$ + DLIN over Bilinear Groups + PRGs in $\text{NC}^0$ + LWE [JLS20]
- LPN over $\mathbb{Z}_p$ + DLIN over Bilinear Groups + PRGs in $\text{NC}^0$ [JLS21]

⚠ Not post-quantum secure (DLIN over Bilinear Groups).
• Multilinear Maps, GGH’15 encodings [GGH+13, GGH15, CVW18], Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20], Split-FHE Paradigm [BDGM20A]

⚠ No reduction to simple, falsifiable assumption.

• Shielded Randomness Leakage (SRL) [GP20, BDGM20B]

⚠ Circuit-dependent hardness assumption: Each circuit being obfuscated gives a different hardness assumption. (Harder to cryptanalyze)

⚠ Explicit counterexample to [GP20] given by [HJL21]. (NOT an attack on obfuscation scheme).

• Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]

⚠ Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.
PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

[GGH+13, GGH15, GJK18, BIJ+20, CVW18, BDGM20A, BDGM20B, GP20, WW20, DQVWW21,...]

- GGH’15 Encodings [GGH+13, GGH15, CVW18], Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BIJ+20], Split FHE Paradigm [BDGM20A]
  - No reduction to simple, falsifiable assumption.

- Shielded Randomness Leakage (SRL) [GP20, BDGM20B]
  - Circuit-dependent hardness assumption: Each circuit being obfuscated gives a different hardness assumption. (Harder to cryptanalyze)
  - Explicit counterexample to [GP20] given by [HJL21]. (NOT an attack on obfuscation scheme).

- Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]
  - Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.

Many beautiful post-quantum iO candidate constructions.

Cryptanalysis refines our assumptions and helps us understand the security. We need to facilitate it.
Many beautiful post-quantum iO candidate constructions.

Cryptanalysis refines our assumptions and helps us understand the security. We need to facilitate it.

Desiderata for Assumptions

✓ Simple-to-state, falsifiable, fully specified.
PLAUSIBLY POST-QUANTUM CONSTRUCTIONS

• GGH’15 Encodings [GGH+13, GGH15, CVW18], Tensor products [GJK18], NLFE [Agr19, AP20], Affine determinant programs [BJ+20], Split-FHE Paradigm [BDGM20A]
  - No reduction to simple, falsifiable assumption.

• Shielded Randomness Leakage (SRL) [GP20, BDGM20B]
  - Circuit-dependent hardness assumption: Each circuit being obfuscated gives a different hardness assumption. (Harder to cryptanalyze)
  - Explicit counterexample to [GP20] given by [HJL21]. (NOT an attack on obfuscation scheme).

• Homomorphic Pseudorandom LWE Samples (HPLS) [WW20]
  - Unspecified circuit implementation of PRF [exploited by [HJL21], (NOT an attack on obfuscation scheme)]. When specifying said circuit, difficult to explicitly write down error-distribution, therefore hard to cryptanalyze.

<table>
<thead>
<tr>
<th>[DQVWW21] Candidate construction via Subspace Flooding Assumption</th>
</tr>
</thead>
<tbody>
<tr>
<td>✓ First fully specified and falsifiable assumption.</td>
</tr>
<tr>
<td>✓ Elegant candidate construction.</td>
</tr>
<tr>
<td>✓ Prior attacks shown to fail.</td>
</tr>
</tbody>
</table>
**SUBSPACE FLOODING ASSUMPTION**

[DQVWW21]

Subspace Flooding Assumption

\[ P, P', seed_{B^*}, A^*, \hat{B} = A^* S_0 + F, C = A^* R + E - bG, E^* + E \cdot G^{-1}(\hat{B}) - bF \]

Hides bit \( b \)

All these givens are matrices drawn from some distribution.

\[ \{B_i = A_i S_i + E_i\}_{i \in [d]} \quad \rightarrow \quad B^* = A^* S^* + E^* \]

\( E^* \), which depends on \( \{E_i\}_{i \in [d]} \), drowns out some a specific error distribution dependent on the bit \( b \).
OUR WORK

**Subspace Flooding Assumption** [DQVWW21]

\[
P, P', \text{seed}_{B^*}, A^*, \hat{B} = A^* S_0 + F, C = A^* R + E - bG, E^* + E \cdot G^{-1}(\hat{B}) - bF
\]

Hides bit \( b \)

**Theorem (informal):** Under a reasonable conjecture, when \( b = 0 \), there exists a PPT algorithm that recovers the \( \{E_i\}_{i \in [d]} \) from the givens.

**Corollary (informal):** Under a heuristic argument, we obtain a PPT distinguisher for the subspace-flooding assumption.
CONJECTURE

$T$ many linearly independent vectors
**CONJECTURE**

$T \ll M$. Conjecture is that these vectors remain linearly independent under left-multiplication by $P$.

Provable under entries from uniform dist. and uniform on $[-B, B]$. 

Entries of $P$ from LWE error distribution (e.g. discrete gaussian).
THE DQVWW21
CONSTRUCTION
APPROACH
To build $iO$, it suffices to build SRE.

SRE $\rightarrow$ $XiO \rightarrow iO$ [LPST16]
SRE SYNTAX

[IK00, IK02, AIK04, BGL+15, LPST16, WW21, DQVWW21]

To build \( iO \), it suffices to build SRE.

\[
\text{SRE} \rightarrow \text{XiO} \rightarrow iO \quad \text{[LPST16]}
\]

\[
f : \{0, 1\}^\ell \rightarrow \{0, 1\}^N
\]

Correctness: \( Enc(f, x) \overset{\text{comp}}{\rightarrow} f(x) \)

Security: \( \forall x_0, x_1, \text{ s.t. } f(x_0) = f(x_1), Enc(f, x_0) \approx_{\text{comp}} Enc(f, x_1) \)

Succinctness: \( |Enc(f, x)| = O(N^\delta), \delta < 1 \)
SRE FROM SUCINCT LWE SAMPLING

\[ f : \{0, 1\}^\ell \to \{0, 1\}^N \]

**Enc**(f, x):

- Generates a large pseudorandom LWE sample of the form \( B^* = A S^* + E^* \)
- Post-evaluation randomness
- Random matrix (flooding)
- Random matrix.
- Homomorphic commitment to x.

(dual GSW)
How do you generate a pseudorandom LWE sample?

\[
\text{seed}_{B^*} \quad \begin{array}{c}
\vdots \\
S^* + E^*
\end{array}
\]
A NATURAL APPROACH: TENSORING

[DQVWW21]
Suppose we knew $Y = A^* S^*$. Do the secrets in the seed remain hidden?

$\text{Known values}$
Suppose we knew $Y = A^* S^*$. Do the secrets in the seed remain hidden?

\begin{align*}
\text{seed}_{B^*} &= \begin{pmatrix}
A_1 & S_1 \\
A_2 & S_2
\end{pmatrix} + \begin{pmatrix}
E_1 \\
E_2
\end{pmatrix} \\
\text{Suppose we knew...}
\end{align*}

\begin{align*}
Y &= \begin{pmatrix}
A_1 & I_m & I_m & A_2
\end{pmatrix} \\
&= \begin{pmatrix}
S_1 & B_2 \\
E_1 & S_2
\end{pmatrix}
\end{align*}

\textcolor{red}{$= \text{Known values}$}
Suppose we knew \( Y \triangleq A^*S^* \) and \( A_1, A_2 \). Can compute left annihilators!

\[
\begin{align*}
\text{seed}_{B^*} & \quad B_1 \\ A_1 & \quad S_1 & + & \quad E_1 \\
B_2 & \quad A_2 & \quad S_2 & + & \quad E_2 \\
\end{align*}
\]
Our Attack (Simplified)

Suppose we knew $Y \triangleq A^* S^*$ and $A_1, A_2$.

...then we can recover $S_1$ by solving an affine system of equations

$B_1 A_1 S_1 + E_1 \neq B_2 A_2 S_2 + E_2$

$= \begin{bmatrix} I_m & \otimes & A_2^\perp \end{bmatrix} \begin{bmatrix} Y \end{bmatrix} = \begin{bmatrix} I_m & \otimes & A_1 \otimes I_m \end{bmatrix} \begin{bmatrix} V_1 \otimes B_2 \end{bmatrix}$

$\color{red} = \text{Known values}$
Suppose we knew $Y \triangleq A^* S^*$ and $A_1, A_2$.

...then we can recover $S_1$ by solving an affine system of equations.

$\color{red}=$ Known values

\[\begin{align*}
Y &= I_m \otimes A_2^\perp + V_1 \otimes B_2 \\
Y &= I_m \otimes A_2^\perp + A_1 \otimes I_m + V_1 \otimes B_2
\end{align*}\]
Suppose we knew $Y \equiv A^* S^*$ and $A_1, A_2$.

...then we can recover $S_1$ by solving an affine system of equations
Suppose we knew $Y \triangleq A^* S^*$ and $A_1, A_2$.

\[ Y = \]

...and then repeat for $S_2$

\[ = \text{Known values} \]
OUR ATTACK (SIMPLIFIED)

If we knew these values, we'd be able to recover the error terms in the seed!

= Known values
**OUR ATTACK (SIMPLIFIED)**

Intended attack to recover components:
1. Recover $A_1, A_2$.
3. Recover $S_1$.
4. Repeat for next index.

---

$\text{seed}_{B^*}$

$B_1$ $A_1$ $S_1$ + $E_1$

$B_2$ $A_2$ $S_2$ + $E_2$

$A_1$ $I_m$ $I_m$ $A_2$

$V_1$ $B_2$

$E_1$ $S_2$

$Y = \begin{array}{c}
\text{? How?} \\
\text{? How?} \\
\text{? How?}
\end{array}$

$\text{Known values} = \begin{array}{c}
\text{? How?} \\
\text{? How?} \\
\text{? How?}
\end{array}$
Can you recover the components $A_1, A_2$ from $A^*$?
UNIQUE REPRESENTATIONS (SIMPLIFIED)

Hypothetical Constraints

$\text{seed}_{B^*}$

Equations

\[ A^* = \begin{bmatrix}
U_1 & I_m \\
I_m & U_2
\end{bmatrix} \]

- Many possible solutions.
- A unique solution is necessary to recover a unique secret.

$\text{Known values}$
UNIQUE REPRESENTATIONS OF $A_i$ (SIMPLIFIED)

Hypothetical Constraints

$\text{seed}_{B^*}$

$B_1$ $U_1$ $V_1$ + $E_1$

$B_2$ $U_2$ $V_2$ + $E_2$

Equations

$A^*$

$A_1$

Corresponding $V_1$ solution:

$S_1$

$U \otimes I_m$ $I_m \otimes U_2$

A possible solution to $U_1$:

$\text{Known values}$
UNIQUE REPRESENTATIONS OF $A_i$ (SIMPLIFIED)

Hypothetical Constraints

$\text{seed}_{B^*}$

$B_1: U_1 V_1 + E_1$

$B_2: U_2 V_2 + E_2$

Equations

$A^*$

$= \begin{bmatrix} U_1 \otimes I_m & I_m \otimes U_2 \end{bmatrix}$

A possible solution to $U_1$:

$A_1 T$

Corresponding $V_1$ solution:

$T^{-1} S_1$

$\text{Known values}$
UNIQUE REPRESENTATIONS OF $A_i$ (SIMPLIFIED)

Hypothetical Constraints

\[ B^* \]

\[
\begin{align*}
B_1 & \quad U_1 \quad V_1 + E_1 \\
B_2 & \quad U_2 \quad V_2 + E_2
\end{align*}
\]

Equations

\[
A^* \quad = \quad \begin{pmatrix}
U_1 \otimes I_m & I_m \otimes U_2
\end{pmatrix}
\]

A possible solution to $U_1$:

\[
\begin{align*}
A_{1,T} & \quad T \\
A_{1,\perp} & \quad S_1
\end{align*}
\]

Corresponding $V_1$ solution:

\[
T^{-1}
\]

\[ \text{Known values} \]
**UNIQUE REPRESENTATIONS OF \( A_i \) (SIMPLIFIED)**

**Hypothetical Constraints**

\[ B_1: U_1 V_1 + E_1 \]

\[ B_2: U_2 V_2 + E_2 \]

**Equations**

\[
\begin{align*}
A^* &= U_1 \otimes I_m \quad \text{or} \quad I_m \otimes U_2 \\
A^* &= \left( A_{1,\top} \right) = 1
\end{align*}
\]

\[ A_{1,\top} \]

**A possible solution to \( U_1 \):**

\[ A_{1,\top}, A_{1,\top}^{-1} \]

**Corresponding \( V_1 \) solution:**

\[ A_{1,\top}, S_1 \]

\( \text{Known values} \)

\[ = \]

38
UNIQUE REPRESENTATIONS OF $A_i$ (SIMPLIFIED)

Hypothetical Constraints

$B_1 \quad U_1 \quad V_1 \quad + \quad E_1$

$B_2 \quad U_2 \quad V_2 \quad + \quad E_2$

Equations

$A^*$

$= U_1 \otimes I_m \quad | \quad I_m \quad \otimes U_2$

For uniqueness, insist on a solution of the form:

$U_1 = I_w \quad \tilde{A}_1$

$= \text{Known values}$
UNIQUE REPRESENTATIONS OF $A_i$ (SIMPLIFIED)

Hypothetical Constraints

$\text{seed}_{B^*}$

$B_1 = \begin{bmatrix} U_1 & V_1 \end{bmatrix} + E_1$

$B_2 = \begin{bmatrix} U_2 & V_2 \end{bmatrix} + E_2$

Equations

$A^* = \begin{bmatrix} U_1 \otimes I_m & I_m \otimes U_2 \end{bmatrix}$

Intended solution to $U_1, V_1$:

$A_{1,\top} A_{1,\top}^{-1} = I_w$

For uniqueness, insist on a solution of the form:

$\color{red} = \text{Known values}$
For uniqueness, insist on a solution of the form:

\[ U_1 = I_w \]

\[ \tilde{A}_1 \]

= Known values

To prove uniqueness, we use a linear independence argument made possible by both the tensoring and the structure of the solutions.
**OUR ATTACK (SIMPLIFIED)**

1. Recover $A_1, A_2$ up to unique representation.
2. Compute $Y = A^*S^*$?
3. Recover $S_1$ up to unique representation.

$\square$ = Known values
Our Attack (Simplified)

From the givens, we can compute:

\[ Y' = A^* \cdot (S^* + R \cdot G^{-1}(\hat{B})) \]

How?

1. Recover \( A_1, A_2 \) up to unique representation.
2. Compute \( Y = A^* S^* \)?
3. Recover \( S_1 \) up to unique representation.

\( \text{seed}_{B^*} \)

\( B_1 \)

\( A_1 \)

\( S_1 \)

\( E_1 \)

\( B_2 \)

\( A_2 \)

\( S_2 \)

\( E_2 \)

\( V_1 \times \)

\( B_2 \)

\( Z \)

\( \text{Known values} \)
Our Attack (Simplified)

1. Recover $A_1, A_2$ up to unique representation.
2. Compute $Y = A^*S^*$?
3. Recover $S_1$ up to unique representation.

From the givens, we can compute:

$$Y' = A^* \cdot (S^* + R \cdot G^{-1}(\hat{B}))$$

$\square$ = Known values

Compute right annihilator $Q$ for $G^{-1}(\hat{B})$
Our Attack (Simplified)

From the givens, we can compute:

\[ Y' \cdot Q = A^* \cdot S^* \cdot Q \]

= Known values

1. Recover \( A_1, A_2 \) up to unique representation.
2. Compute \( Y = A^* S^* Q \).
3. Recover \( S_1 \) up to unique representation.
Our Attack (Simplified)

Seed: $\text{seed}_{B^*}$

1. Recover $A_1, A_2$ up to unique representation.
2. Compute $Y = A^* S^* Q$.
3. Recover $S_1$ up to unique representation.

From the givens, we can compute:

$$Y' \cdot Q = A^* \cdot S^* \cdot Q$$

= Known values
Our Attack (Simplified)

From the givens, we can compute:

\[ Y' \cdot Q = A^* \cdot S^* \cdot Q \]

Recover \( A_1, A_2 \) up to unique representation.

Compute \( Y = A^*S^*Q \).

Recover \( S_1 \) up to unique representation.
OUR ATTACK (SIMPLIFIED)

\[ Y = A_1 \otimes I_m \otimes A_2 \]

Expand above:

\[ Y'' = A'' X_1 + B'' X_2 \]

- Recover \( A_1, A_2 \) up to unique representation.
- Compute \( Y = A^* S^* Q \).
- Recover \( S_1 \) up to unique representation.

\( \text{seed}_{B^*} \)

\( B_1: A_1 \boxplus S_1 + E_1 \)

\( B_2: A_2 \boxplus S_2 + E_2 \)

\( = \) Known values
**OUR ATTACK (SIMPLIFIED)**

- **Seed** $B^*$
- **Known Values**

Generically, want to show that $X_1$ has unique solutions:

$$Y'' = A'' X_1 + B'' X_2$$

...involves analyzing overlap in column span of $A''$ and $B''$

- Recover $A_1, A_2$ up to unique representation.
- Compute $Y = A^* S^* Q$.
- Recover $S_1$ up to unique representation.

$= \text{Known values}$
BREAKING THE FULL ASSUMPTION

\[ P, P', \text{seed}_{B^*}, A^*, \hat{B} = A^*S_0 + F, \quad C = A^*R + E - bG, \quad E^* + E \cdot G^{-1}(\hat{B}) - bF \]

Several randomization tricks were used in the construction in [DQVWW21].
BREAKING THE FULL ASSUMPTION

\[ P, P', \text{seed}_{B^*}, A^*, \hat{B} = A^*S_0 + F, C = A^*R + E - bG, E^* + E \cdot G^{-1}(\hat{B}) - bF \]

Several randomization tricks were used in the construction in [DQVWW21].

**Final Remark 1:** Under a reasonable conjecture on \( P \) preserving rank of small subspaces, the toy analysis given extends to when \( P \) and \( P' \) are present.
BREAKING THE FULL ASSUMPTION

\[ P, P', \text{seed}_{B^*}, A^*, \hat{B} = A^*S_0 + F, C = A^*R + E - bG, E^* + E \cdot G^{-1}(\hat{B}) - bF \]

Several randomization tricks were used in the construction in [DQVWW21].

**Final Remark 1:** Under a reasonable conjecture on \( P \) preserving rank of small subspaces, the toy analysis given extends to when \( P \) and \( P' \) are present.

**Final Remark 2:** We show that Kilian randomization on \( A^*, S^* \) does not hide the tensor structure.
BREAKING THE FULL ASSUMPTION

\[ P, P', \text{seed}_{B^*}, A^* , \hat{B} = A^*S_0 + F, C = A^*R + E - bG, E^* + E \cdot G^{-1}(\hat{B}) - bF \]

Several randomization tricks were used in the construction in [DQVWW21].

**Final Remark 1:** Under a reasonable conjecture on \( P \) preserving rank of small subspaces, the toy analysis given extends to when \( P \) and \( P' \) are present.

**Final Remark 2:** We show that Kilian randomization on \( A^* , S^* \) does not hide the tensor structure.

**Final Remark 3:** We show that the attack extends to the “\( T \)-sum” candidate construction in [DQVWW21]
THANK YOU!