

از مبهم سازی ارتقاء NC^1 به $P/poly$ تابعی رمز گذاری و

فرشیم پویا

سوپرپور نورمال اکول – بلفاست کوئینز دانشگاه

رمز مبانی – کامپیوتری علوم ریاضی جنبه های



Bootstrapping iO from NC^1 to P/poly and Functional Encryption

Pooya Farshim

Queen's University Belfast/École Normale Supérieure

Mathematical Aspects of Computer Science – Foundations of Cryptography



Breakthrough Result of 2013

Candidate Indistinguishability Obfuscation and Functional Encryption for all circuits

Sanjam Garg
UCLA
sanjamg@cs.ucla.edu

Craig Gentry
IBM Research
craigbgentry@gmail.com

Shai Halevi
IBM Research
shaih@alum.mit.edu

Mariana Raykova
IBM Research
mariana@cs.columbia.edu

Amit Sahai
UCLA
sahai@cs.ucla.edu

Brent Waters
University of Texas at Austin
bwaters@cs.utexas.edu

July 21, 2013

Abstract

In this work, we study *indistinguishability obfuscation* and *functional encryption* for general circuits:

Indistinguishability obfuscation requires that given any two equivalent circuits C_0 and C_1 of similar size, the obfuscations of C_0 and C_1 should be computationally indistinguishable.

In functional encryption, ciphertexts encrypt inputs x and keys are issued for circuits C . Using the key SK_C to decrypt a ciphertext $CT_x = \text{Enc}(x)$, yields the value $C(x)$ but does not reveal anything else about x . Furthermore, no collusion of secret key holders should be able to learn anything more than the union of what they can each learn individually.

We give constructions for indistinguishability obfuscation and functional encryption that supports all polynomial-size circuits. We accomplish this goal in three steps:

- We describe a candidate construction for indistinguishability obfuscation for NC^1 circuits. The security of this construction is based on a new algebraic hardness assumption. The candidate and assumption use a simplified variant of multilinear maps, which we call *Multilinear Jigsaw Puzzles*.
- We show how to use indistinguishability obfuscation for NC^1 together with Fully Homomorphic Encryption (with decryption in NC^1) to achieve indistinguishability obfuscation for all circuits.
- Finally, we show how to use indistinguishability obfuscation for circuits, public-key encryption, and non-interactive zero knowledge to achieve functional encryption for all circuits. The functional encryption scheme we construct also enjoys succinct ciphertexts, which enables several other applications.

Indistinguishability Obfuscation (iO)

Security: Recall iO security:

$$\text{iO}(C_0) \stackrel{c}{\approx} \text{iO}(C_1) .$$

for **functionally equivalent** C_0 and C_1 .

$\text{IND}_{\text{Obf}}^{\mathcal{S}, \mathcal{A}}(1^\lambda):$ $b \leftarrow \$ \{0, 1\}$ $(C_0, C_1, st) \leftarrow \$ \mathcal{S}(1^\lambda)$ $\bar{C} \leftarrow \$ \text{Obf}(1^\lambda, C_b)$ $b' \leftarrow \$ \mathcal{A}(1^\lambda, st)$ return $(b = b')$	$\text{Eq}_{\mathcal{S}}^{\mathcal{D}}(1^\lambda):$ $(C_0, C_1, st) \leftarrow \$ \mathcal{S}(1^\lambda)$ $x \leftarrow \$ \mathcal{D}(C_0, C_1, st)$ return $(C_0(x) \neq C_1(x))$
---	--

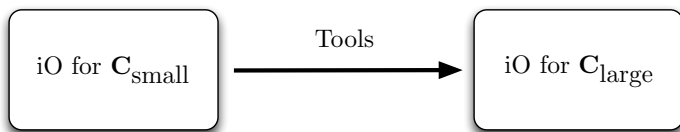
Sampler $\mathcal{S}$ is Eq-secure if for all (even unbounded) $\mathcal{D}$

$$\Pr \left[\text{Eq}_{\mathcal{S}}^{\mathcal{D}}(1^\lambda) \right] \in \text{Negl} .$$

Security for all Eq-secure ppt $\mathcal{S}$ and all ppt $\mathcal{A}$

$$\text{Adv}_{\text{Obf}, \mathcal{S}, \mathcal{A}}^{\text{ind}}(\lambda) := 2 \cdot \Pr \left[\text{IND}_{\text{Obf}}^{\mathcal{S}, \mathcal{A}}(1^\lambda) \right] - 1 \in \text{Negl} .$$

Bootstrapping



For us:

$$C_{\text{small}} = \mathbf{NC}^1 \quad \text{and} \quad C_{\text{large}} = \mathbf{P}/\text{poly}$$

Tools:

- Fully homomorphic encryption with $\text{Dec}(\cdot, C) \in C_{\text{small}}$.
- Low-depth proofs with verification in C_{small} .

iO for $\mathbf{NC}^1$: See Mohammad's talk next!

Nick's Class

NC^1 looks something like:

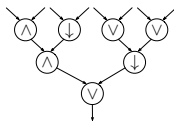
$d(2) = 1$



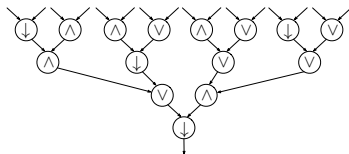
$d(4) = 2$



$d(8) = 3$

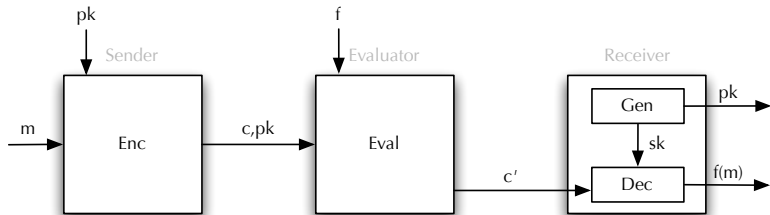


$d(16) = 4$



- $\text{NC}^i :=$ circuit families C_λ with constant fan-in/out gates whose depth grow like $\mathcal{O}(\log^i(\lambda))$ with input size λ .
- $\text{P/poly} := \bigcup_{c \in \mathbb{N}} \{ \text{circuit families whose size grow like } \mathcal{O}(\lambda^c) \}$.

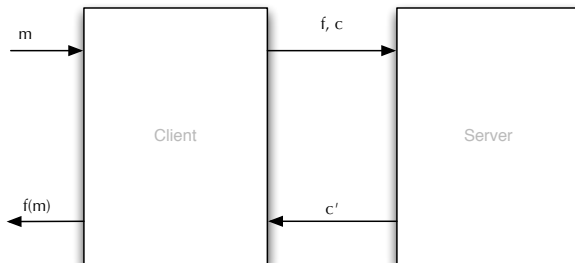
Fully Homomorphic Encryption (FHE)



Scheme is:

Fully homomorphic if it supports all $f \in \mathbf{P}/\text{poly}$.
 $L(\lambda)$ -leveled homomorphic if it supports all $f \in \mathbf{NC}^{L(\cdot)}$.

Outsourcing of Computation



FHE Details

- 1 $\text{Gen}(1^\lambda)$ outputs key-pair (sk, pk)
- 2 $\text{Enc}(pk, m)$ outputs ciphertext c .
- 3 $\text{Eval}(pk, f, c_1, \dots, c_n)$ outputs ciphertext c .
- 4 $\text{Dec}(sk, c)$ outputs a message m .

Correctness: If $c_1, \dots, c_n$ encrypt $m_1, \dots, m_n$:

$$\text{Dec}(sk, \text{Eval}(pk, f, c_1, \dots, c_n)) = f(m_1, \dots, m_n) .$$

Compactness:

$$|\text{Eval}(pk, f, c_1, \dots, c_n)| \text{ depends on } \lambda \text{ only.}$$

Security:

$$(pk, \text{Enc}(pk, m_0)) \stackrel{c}{\approx} (pk, \text{Enc}(pk, m_1))$$

The Bootstrapping Step

Intuition:

$\text{Obf}(F)$: output $c \leftarrow_{\$} \text{Enc}(pk, F)$ and an obfuscation $\overline{\text{Dec}}$ of $\text{Dec}(sk, \cdot)$.

How can we run $\text{Obf}(F)(x)$?

Evaluate $c' := \text{Eval}(pk, \text{UC}(\cdot, x), c)$ and then return $\overline{\text{Dec}}(c')$

We'll use the Naor–Yung paradigm [NY90] to make sure $\overline{\text{Dec}}$ hides sk :

Doubly encrypt F and require **consistency** across **two** evaluations.

Details

- Generate two keys $(sk_i, pk_i) \leftarrow_{\$} \text{Gen}(1^\lambda)$ for $i = 1, 2$
- Encrypt $G_i \leftarrow_{\$} \text{Enc}(pk_i, F)$ for $i = 1, 2$
- Generate $\bar{P}$ as an NC^1 obfuscation of:

$$P[sk_1](m, E_1, E_2, \pi) := \text{if } V((m, E_1, E_2), \pi) \text{ ret. Dec}(sk_1, E_1) \\ \text{else return } \perp$$

- Return $(\bar{P}, pk_1, pk_2, G_1, G_2)$

What's V ? A low-depth proof of consistency that

$$\begin{aligned} \exists (G_1, G_2) : \quad & E_1 = \text{Eval}(pk_1, \text{UC}(\cdot, m), G_1) \\ & \wedge \quad E_2 = \text{Eval}(pk_2, \text{UC}(\cdot, m), G_2) \end{aligned}$$

Low-Depth Proof System (P, V) for Relation R

Perfect Completeness : For all (x, w) with $R(x, w) = 1$

$$\Pr[\pi \leftarrow_{\$} P(x, w) : V(x, \pi) = 1] = 1 .$$

Perfect Soundness : For all $x \notin R$ and for all (even unbounded) P^*

$$\Pr[\pi \leftarrow_{\$} P^*(x) : V(x, \pi) = 1] = 0 .$$

The proof is **low depth** if

$$V(\cdot, \cdot) \in \mathbf{NC}^1$$

Construction:

$P(x, w) :=$ List of all internal wire values of $R(x, w)$

$V(x, \pi) :=$ Check if all wire values in π are consistent wrt. input x

Proof of Security

Our goal is to prove:

$$\text{Obf}(C_0) \stackrel{c}{\approx} \text{Obf}(C_1)$$

$$\left(\underbrace{\text{Enc}(pk_1, C_0)}_{G_1}, \underbrace{\text{Enc}(pk_2, C_0)}_{G_2}, P[sk_1] \right) \stackrel{c}{\approx} \left(\underbrace{\text{Enc}(pk_1, C_1)}_{G_1}, \underbrace{\text{Enc}(pk_2, C_1)}_{G_2}, P[sk_1] \right)$$

Game	G_1 contains	G_2 contains	$P[sk]$ knows	Remark
0	C_0	C_0	sk_1	iO Game wrt. C_0
1	C_0	C_1	sk_1	IND-CPA wrt. pk_2
2	C_0	C_1	sk_2	iO for $\text{NC}^1 + \underbrace{P[sk_1] \equiv P[sk_2]}_{\text{Correctness} + \pi + (C_0 \equiv C_1)}$
3	C_1	C_1	sk_2	IND-CPA wrt. pk_1
4	C_1	C_1	sk_1	NC^1 iO + $P[sk_2] \equiv P[sk_1]$
	C_1	C_1	sk_1	iO Game wrt. C_1

Why is $\overline{\mathcal{S}}$ Eq-secure?

Need to show:

$$P[sk_1] \equiv P[sk_2]$$

Recall:

$$P[sk_1](m, E_1, E_2, \pi) := \text{if } V((m, E_1, E_2), \pi) \text{ ret. Dec}(sk_1, E_1) \\ \text{else return } \perp$$

This follows from:

- Proof π says E_1 and E_2 are correctly evaluated.
- The proof system is **perfectly** sound.
- FHE is **perfectly** correct.
- Circuits C_0 and C_1 are functionally equivalent.

Applications of iO

Functional Encryption (FE)

$$\begin{aligned}(msk, mpk) &\leftarrow \$ \text{Setup}(1^\lambda) \\ TK_f &\leftarrow \$ \text{TKGen}(msk, f) \\ c &\leftarrow \$ \text{Enc}(mpk, m) \\ f(m)/\perp &= \text{Dec}(c, TK_f)\end{aligned}$$

What can I do with an FE for $f = id$ only? PKE!

Attribute-Based Encryption

Fine-grained access to encrypted data.

$$f[P_\alpha](\underbrace{A, M}_m) := \begin{cases} m & \text{if } P_\alpha(A) = 1 ; \\ \perp & \text{otherwise.} \end{cases}$$

For instance:

- Consider policies P_α

$$P_\alpha(A) := (\alpha \geq A)$$

- TA checks users' age $\alpha \in [100]$ and issues TK_{P_α}
- Now if a user has $\text{Enc}(mpk, (18, M))$ it can decrypt it with key $TK_{P_{19}}$ but not with $TK_{P_{17}}$: only adults can see M .

FE Security

Intuition: Requires that:

$$\text{Enc}(m_0) \stackrel{c}{\approx} \text{Enc}(m_1)$$

In the presence of $TK_{f_1}, \dots, TK_{f_n}$, as long as $f_i(m_0) = f_i(m_1)$ for all i .

$\text{IND-CPA}_{\text{FE}}^A(1^\lambda):$ $(msk, mpk) \leftarrow \$ \text{Setup}(1^\lambda)$ $(m_0, m_1, st) \leftarrow \$ \mathcal{A}_1^{\text{TOKEN}}(mpk)$ $b \leftarrow \$ \{0, 1\}$ $c \leftarrow \$ \text{Enc}(mpk, m_b)$ $b' \leftarrow \$ \mathcal{A}_2^{\text{TOKEN}}(c, st)$ return $(b = b')$	$\text{TOKEN}(f):$ $TK \leftarrow \$ \text{TKGen}(msk, f)$ $\text{TKList} \leftarrow \text{TKList} : f$ return TK
---	--

Legitimacy:

$$\forall f \in \text{TKList} : f(m_0) = f(m_1) .$$

Advantage:

$$\text{Adv}_{\text{FE}, \mathcal{A}}^{\text{ind-cpa}}(\lambda) := 2 \cdot \Pr \left[\text{IND-CPA}_{\text{FE}}^A(1^\lambda) \right] - 1$$

The iO-to-FE Transform

Intuition:

$\text{Setup}(1^\lambda)$: $msk = sk$ and $mpk = pk$.

$\text{Enc}(mpk, m)$: Encrypt using $\text{PKEnc}(pk, m)$.

$\text{TKGen}(msk, f)$: $TK_f = \text{Obfuscation of } f(\text{PKDec}(sk, \cdot))$.

$\text{Dec}(TK_f, c)$: Run TK_f on c .

To “switch” keys/messages in the reduction, attach proofs of consistency.

FE Construction – Details

$\text{Setup}(1^\lambda)$: Set $\text{mpk} := (pk_1, pk_2, \sigma)$ and $\text{msk} = sk_1$.

$\text{Enc}(\text{mpk}, m)$: Output $E_1 \leftarrow_{\$} \text{PKEnc}(pk_1, m)$ and $E_2 \leftarrow_{\$} \text{PKEnc}(pk_2, m)$,
and a **NIZK proof** π of well-formedness:

$$\begin{aligned} \exists (m, r_1, r_2) : E_1 &= \text{PKEnc}(pk_1, m; r_1) \\ &\wedge E_2 = \text{PKEnc}(pk_2, m; r_2) \end{aligned}$$

$\text{TKGen}(\text{msk}, f)$: Output an obfuscation of:

$$\begin{aligned} P[sk_1, f, \sigma](E_1, E_2, \pi) &:= \text{if } V(\sigma, (E_1, E_2), \pi) \text{ ret. } f(\text{PKDec}(sk_1, E_1)) \\ &\text{else return } \perp \end{aligned}$$

$\text{Dec}(c, \text{TK}_f)$: Run TK_f on $c = (E_1, E_2, \pi)$.

Non-Interactive Zero-Knowledge Proofs

A NIZK for NP relation R is a ppt triple (K, P, V) such that:

Perfect Completeness : For all (x, w) with $R(x, w) = 1$

$$\Pr[\sigma \leftarrow_{\$} K(1^\lambda); \pi \leftarrow_{\$} P(\sigma, x, w) : V(\sigma, x, \pi) = 1] = 1$$

Statistical Soundness : For all (even unbounded) P^*

$$\Pr[\sigma \leftarrow_{\$} K(1^\lambda); \pi \leftarrow_{\$} P^*(\sigma) : V(\sigma, x, \pi) = 1 \wedge x \notin R] \in \text{Negl}$$

Computational ZK : There is a $\mathcal{S} = (\mathcal{S}_1, \mathcal{S}_2)$ st. for all ppt $\mathcal{A}$ and all $x \in R$

$$\begin{aligned} & \Pr[\sigma \leftarrow_{\$} K(1^\lambda); \pi \leftarrow_{\$} P(\sigma, x, w) : \mathcal{A}(\sigma, x, \pi) = 1] \\ & \stackrel{c}{\approx} \Pr[(\sigma, \tau) \leftarrow_{\$} \mathcal{S}_1(1^\lambda, x); \pi \leftarrow_{\$} \mathcal{S}_2(\sigma, x, \tau) : \mathcal{A}(\sigma, x, \pi) = 1] \end{aligned}$$

Statistical Simulation Soundness

Stat. Sim. Soundness : For all (even unbounded) P^* and $x \in R$

$$\Pr[(\sigma, \tau) \leftarrow_{\$} \mathcal{S}_1(1^\lambda, x); \pi \leftarrow_{\$} \mathcal{S}_2(\sigma, x, \tau); (\sigma', \pi') \leftarrow_{\$} P^*(\sigma, x, \pi) : \\ : x \neq x' \wedge V(\sigma, x', \pi') = 1 \wedge x' \notin R] \in \text{Negl}$$

Proof of Security

Game	σ, π	E_1 contains	E_2 contains	$P[sk, f_i]$ knows	$P[sk, f_{i+1}]$ knows	Remark
0	Real	m_0	m_0	sk_1	sk_1	IND-CPA for m_0
1	Sim	m_0	m_0	sk_1	sk_1	Zero Knowledge
2	Sim	m_0	m_1	sk_1	sk_1	IND-CPA wrt. pk_2
$(3, i)$	Sim	m_0	m_1	sk_2	sk_1	iO + SSS
$(3, q)$	Sim	m_0	m_1	sk_2	sk_2	$i = q$
4	Sim	m_1	m_1	sk_2	sk_2	IND-CPA wrt. pk_1
$(5, i)$	Sim	m_1	m_1	sk_1	sk_2	iO + SSS
$(5, q)$	Sim	m_1	m_1	sk_1	sk_1	$i = q$
6	Real	m_1	m_1	sk_1	sk_1	Zero Knowledge IND-CPA for m_1

Details: Game $(3, i) \longrightarrow \text{Game } (3, i + 1)$

Legitimacy requires:

$$P[sk_1, f_{i+1}, \sigma] \equiv P[sk_2, f_{i+1}, \sigma]$$

Let (E_1, E_2, π) be an input:

- Verification of π fails: Both circuits output $\perp$
- Verification passes:
 - ▶ E_1 and E_2 valid (encrypt the same message m). Both output $f_{i+1}(m)$.
 - ▶ E_1 and E_2 are **not** valid.
SSS $\implies E_1$ and E_2 are identical to challenge ciphertexts.
By the rules of FE game $f_{i+1}(m_0) = f_{i+1}(m_1)$.

Other Applications of iO

- Witness Encryption
- Deniable Encryption
- Constrained PRFs
- Symmetric-to-asymmetric conversions
- UCE-secure hash functions
- ...

Thank you.