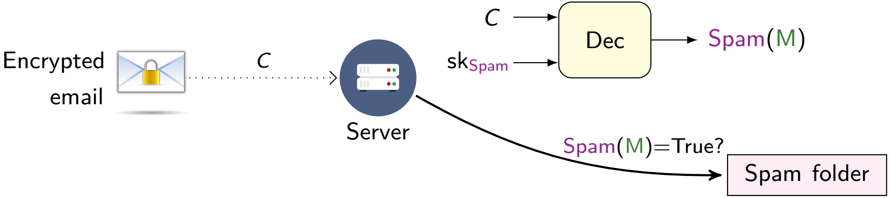
Multi-Input Functional Encryption for Inner Products: Function-Hiding Realizations and Constructions without Pairings

Michel Abdalla Dario Catalano Dario Fiore
Romain Gay Bogdan Ursu

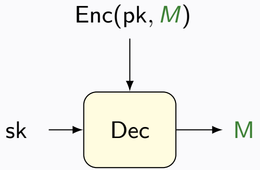
August 21, 2018

Motivation - Spam Server

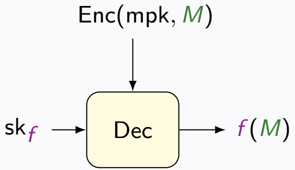


Beyond Public Key Encryption

Public key encryption [Diffie, Hellman 76]

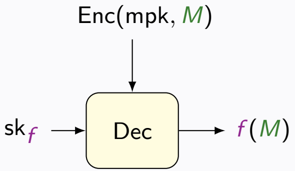


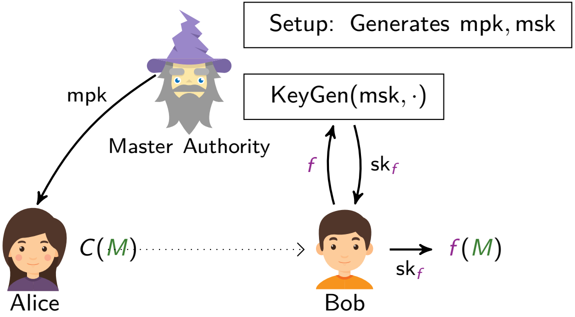
Functional encryption [Boneh, Sahai, Waters 11]



Functional Encryption

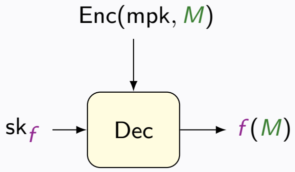
Functional encryption [Boneh, Sahai, Waters 11]





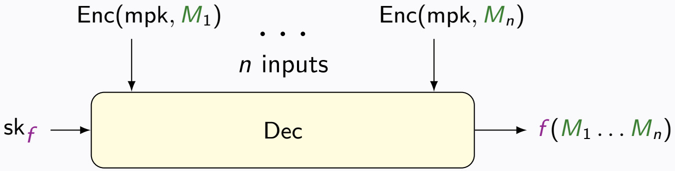
Multi-Input Functional Encryption

Functional encryption



Multi-input functional encryption

[Goldwasser, Gordon, Goyal, Jain, Katz, Liu, Sahai, Shi, Zhou 14]



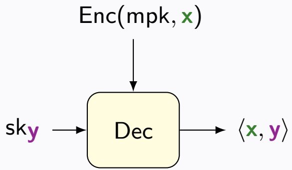
Independent ciphertexts

Inner-Product Functional Encryption

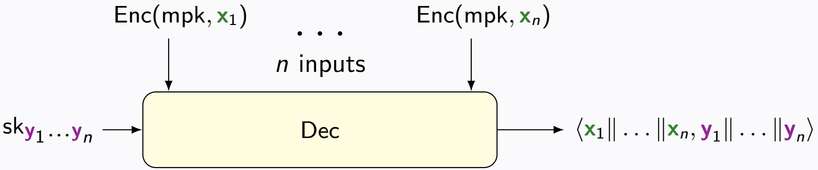
$f_{\mathbf{y}}(\cdot) = \langle \cdot, \mathbf{y} \rangle$

$$f_{\mathbf{y}_1\|\ldots\|\mathbf{y}_n}(\cdot, \ldots, \cdot) = \langle \mathbf{x}_1 \| \ldots \| \mathbf{x}_n, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n \rangle$$

Inner-Product Functional encryption



Multi-input Inner-Product



Independent ciphertexts

Previous Work

Multi-input scheme	Classes of functions	Assumptions
[GGG+14, BLR+15, BGJS15] [AJ15, BKS16] FH	General functions	IO, Multilinear maps, ...

[AGRW17]	Inner products, poly inputs	SXDH in Pairing Groups
[DOT18] FH	Inner products unbounded poly inputs	SXDH in Pairing Groups

FH - function hiding

Previous Work + Our Contribution

Multi-input scheme	Classes of functions	Assumptions
[GGG+14, BLR+15, BGJS15] [AJ15, BKS16] FH	General functions	IO, Multilinear maps, ...
[AGRW17]	Inner products, poly inputs	SXDH in Pairing Groups
[DOT18] FH	Inner products unbounded poly inputs	SXDH in Pairing Groups
This work	Inner products, poly inputs	DDH, DCR or LWE
This work FH	Inner products, poly inputs	SXDH in Pairing Groups

FH - function hiding

Previous Work + Our Contribution

Multi-input scheme	Classes of functions	Assumptions
[GGG+14, BLR+15, BGJS15] [AJ15, BKS16] FH	General functions	IO, Multilinear maps, ...

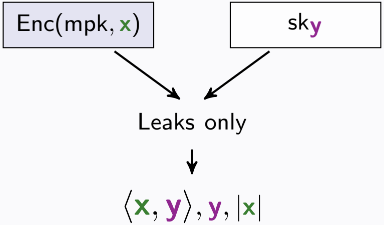
[AGRW17]	Inner products, poly inputs	SXDH in Pairing Groups
[DOT18] FH	Inner products unbounded poly inputs	SXDH in Pairing Groups

This work	Inner products, poly inputs	DDH, DCR or LWE
This work FH	Inner products, poly inputs	SXDH in Pairing Groups

FH - function hiding

Security Goal

Security goal



Security of Multi-Input Functional Encryption

Security goal

$\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_1) \ldots \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_n)$

$\mathsf{sk}_{\mathbf{y}_1 \| \ldots \| \mathbf{y}_n}$

Leaks only

$$\langle \mathbf{x}_1 \| \ldots \| \mathbf{x}_n, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n \rangle, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n, \{|\mathbf{x}_i|\}$$

Security of Multi-Input Functional Encryption

Security goal

$\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_1) \ldots \mathsf{Enc}(\mathsf{mpk}, \mathbf{x}_n)$

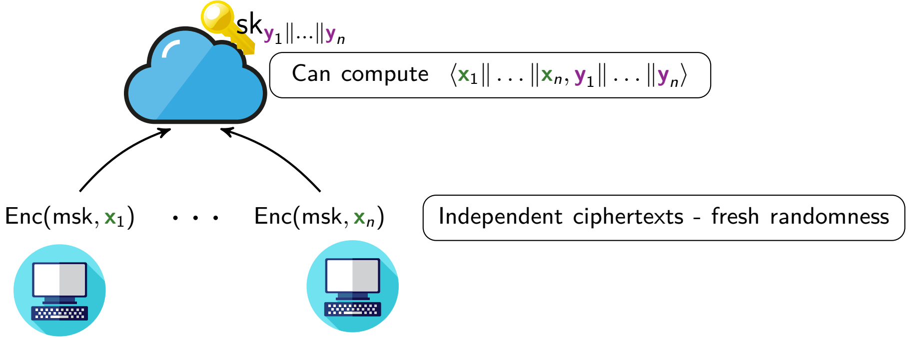
$\mathsf{sk}_{\mathbf{y}_1 \| \ldots \| \mathbf{y}_n}$

Leaks only

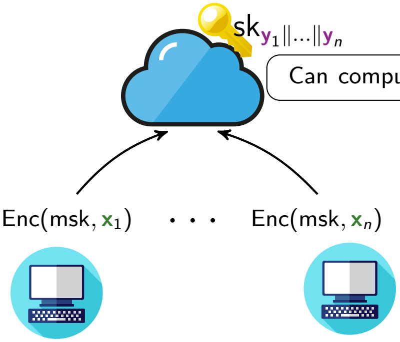
$$\langle \mathbf{x}_1 \| \ldots \| \mathbf{x}_n, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n \rangle, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n, \{|\mathbf{x}_i|\}$$

Leakage is more complex!

Multi-Input Inner-Product Encryption



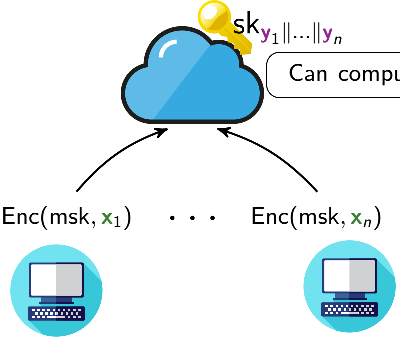
Multi-Input Inner-Product Encryption



Can compute $\langle \mathbf{x}_1\| \ldots \|\mathbf{x}_n, \mathbf{y}_1\| \ldots \|\mathbf{y}_n \rangle$

But nothing more about $\langle \mathbf{x}_i, \mathbf{y}_i \rangle$

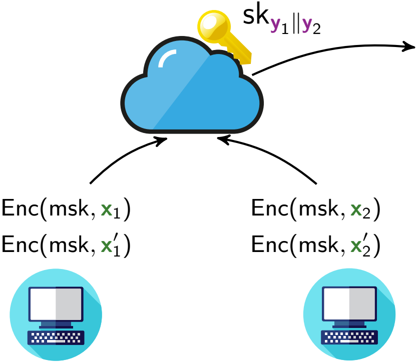
Public Key - Symmetric Key



Can compute $\langle \mathbf{x}_1 \| \ldots \| \mathbf{x}_n, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n \rangle$

But nothing more about $\langle \mathbf{x}_i, \mathbf{y}_i \rangle$
Public key, encrypt $\mathbf{0}$

$$\langle \mathbf{0} \ldots \mathbf{0} \| \mathbf{x}_i \| \mathbf{0} \ldots \mathbf{0}, \mathbf{y}_1 \| \ldots \| \mathbf{y}_n \rangle = \langle \mathbf{x}_i, \mathbf{y}_i \rangle$$

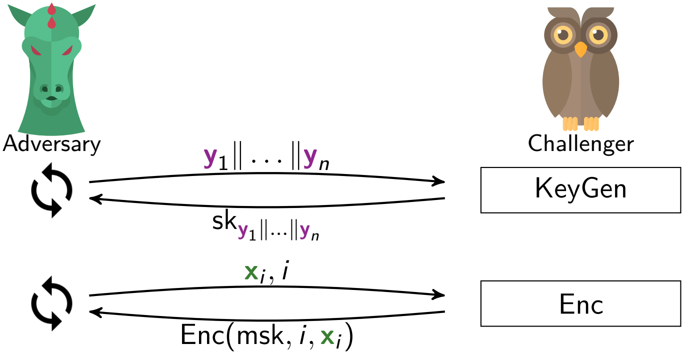


Can compute:
- $\langle \mathbf{x}_1 \| \mathbf{x}_2, \mathbf{y}_1 \| \mathbf{y}_2 \rangle$
- $\langle \mathbf{x}'_1 \| \mathbf{x}_2, \mathbf{y}_1 \| \mathbf{y}_2 \rangle$
- $\langle \mathbf{x}_1 \| \mathbf{x}'_2, \mathbf{y}_1 \| \mathbf{y}_2 \rangle$
- $\langle \mathbf{x}'_1 \| \mathbf{x}'_2, \mathbf{y}_1 \| \mathbf{y}_2 \rangle$

Example for $n = 2$

Difficulty: Allow ciphertext mixing but not key mixing!!!.

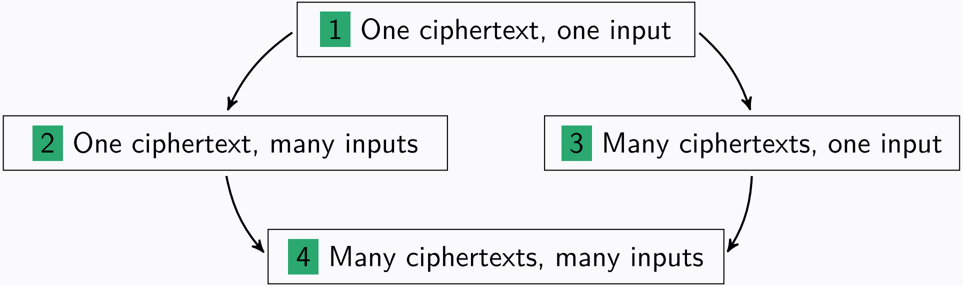
Multi-Input Inner-Product - Security



Adversary only learns $\langle \mathbf{x}_1 \| \dots \| \mathbf{x}_n, \mathbf{y}_1 \| \dots \| \mathbf{y}_n \rangle$ for all queried $(\mathbf{x}_i, i)$ and all queried $\mathbf{y}_1 \| \dots \| \mathbf{y}_n$.

Construction without Pairings

Roadmap



Symmetric setting one ciphertext $\not\Rightarrow$ many ciphertexts

1 One ciphertext, one input

$$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$$

1 One ciphertext, one input

$$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$$

Decrypt with $\mathsf{sk}_{\mathbf{y}}$:

$$\langle \mathbf{x} + \mathbf{u}, \mathbf{y} \rangle - \langle \mathbf{u}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \cancel{\langle \mathbf{u}, \mathbf{y} \rangle} - \cancel{\langle \mathbf{u}, \mathbf{y} \rangle}$$

1 One ciphertext, one input

$$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$$

Decrypt with $\mathsf{sk}_{\mathbf{y}}$:

$$\langle \mathbf{x} + \mathbf{u}, \mathbf{y} \rangle - \langle \mathbf{u}, \mathbf{y} \rangle = \langle \mathbf{x}, \mathbf{y} \rangle + \cancel{\langle \mathbf{u}, \mathbf{y} \rangle} - \cancel{\langle \mathbf{u}, \mathbf{y} \rangle}$$

Security:

$$(\mathbf{x} + \mathbf{u}, \langle \mathbf{u}, \mathbf{y} \rangle, \mathbf{y}) \equiv (\mathbf{w}, \langle \mathbf{w}, \mathbf{y} \rangle - \langle \mathbf{x}, \mathbf{y} \rangle, \mathbf{y})$$

Goal: only leakage on $\mathbf{x}$ is $\langle \mathbf{x}, \mathbf{y} \rangle$. ✓

2 One ciphertext, many inputs

1 One ciphertext, one input

$$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$$
$$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$$

2 One ciphertext, many inputs

$$\mathsf{msk} = \mathbf{u}_1 \ldots \mathbf{u}_n \in \mathbb{Z}_q^{n \times m}$$
$$\mathsf{Enc}_2(\mathsf{msk}, i, \mathbf{x}_i) = \mathbf{x}_i + \mathbf{u}_i \in \mathbb{Z}_q^m$$
$$\mathsf{KeyGen}_2(\mathsf{msk}, \mathbf{y}_1 \ldots \mathbf{y}_n) = \sum_{i=1}^n \langle \mathbf{u}_i, \mathbf{y}_i \rangle \in \mathbb{Z}_q, \mathbf{y}_1 \ldots \mathbf{y}_n$$

1 One ciphertext, one input	2 One ciphertext, many inputs
$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$	$\mathsf{msk} = \mathbf{u}_1 \dots \mathbf{u}_n \in \mathbb{Z}_q^{n \times m}$
$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$	$\mathsf{Enc}_2(\mathsf{msk}, i, \mathbf{x}_i) = \mathbf{x}_i + \mathbf{u}_i \in \mathbb{Z}_q^m$
$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$	$\mathsf{KeyGen}_2(\mathsf{msk}, \mathbf{y}_1 \dots \mathbf{y}_n) = \sum_{i=1}^n \langle \mathbf{u}_i, \mathbf{y}_i \rangle \in \mathbb{Z}_q, \mathbf{y}_1 \dots \mathbf{y}_n$

Dec: $\sum_{i=1}^n \langle \mathbf{x}_i + \mathbf{u}_i, \mathbf{y}_i \rangle - \sum_{i=1}^n \langle \mathbf{u}_i, \mathbf{y}_i \rangle = \langle \mathbf{x}_1 \dots \mathbf{x}_n, \mathbf{y}_1, \dots \mathbf{y}_n \rangle$

3 Many ciphertexts, one input

1 One ciphertext, one input	3 Many ciphertexts, one input [ABDP15]
$\mathsf{msk} = \mathbf{u} \in \mathbb{Z}_q^m$	$\mathsf{msk} = \mathbf{v} \in \mathbb{Z}_q^m$
$\mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) = \mathbf{x} + \mathbf{u} \in \mathbb{Z}_q^m$	$\mathsf{Enc}_3(\mathsf{msk}, \mathbf{x}) = g^r, g^{\mathbf{x}+r\mathbf{v}} \in \mathbb{G}^{m+1}$
$\mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{u}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$	$\mathsf{KeyGen}_3(\mathsf{msk}, \mathbf{y}) = \langle \mathbf{v}, \mathbf{y} \rangle \in \mathbb{Z}_q, \mathbf{y}$

$\mathbb{G}$ prime group of order q

Using [ALS16], this step can also be based on LWE or DCR.

Construction without Pairings

1 One ciphertext, one input

$$\begin{aligned} \mathsf{msk} &= \mathbf{u} \\ \mathsf{Enc}_1(\mathsf{msk}, \mathbf{x}) &= \mathbf{x} + \mathbf{u} \\ \mathsf{KeyGen}_1(\mathsf{msk}, \mathbf{y}) &= \langle \mathbf{u}, \mathbf{y} \rangle, \mathbf{y} \end{aligned}$$

2 One ciphertext, many inputs

$$\begin{aligned} \mathsf{msk} &= \mathbf{u}_1 \dots \mathbf{u}_n \\ \mathsf{Enc}_2(\mathsf{msk}, i, \mathbf{x}_i) &= \mathbf{x}_i + \mathbf{u}_i \\ \mathsf{KeyGen}_2(\mathsf{msk}, \mathbf{y}_1 \dots \mathbf{y}_n) &= \\ \textstyle\sum_{i=1}^{n} \langle \mathbf{u}_i, \mathbf{y}_i \rangle, \mathbf{y}_1 \dots \mathbf{y}_n \end{aligned}$$

3 Many ciphertexts, one input

$$\begin{aligned} \mathsf{msk} &= \mathbf{v} \\ \mathsf{Enc}_3(\mathsf{msk}, \mathbf{x}) &= g^r, g^{\mathbf{x}+r\mathbf{v}} \in \mathbb{G}^{m+1} \\ \mathsf{KeyGen}_3(\mathsf{msk}, \mathbf{y}) &= \langle \mathbf{v}, \mathbf{y} \rangle, \mathbf{y} \end{aligned}$$

4 Many ciphertexts, many inputs

$$\begin{aligned} \mathsf{msk} &= \mathbf{u}_i, \mathbf{v}_i \\ \mathsf{Enc}_4(\mathsf{msk}, i, \mathbf{x}) &= \mathsf{Enc}_3(\mathsf{Enc}_2(\mathsf{msk}, i, \mathbf{x}_i)) \\ \mathsf{KeyGen}_4(\mathsf{msk}, \mathbf{y}_1 \dots \mathbf{y}_n) &= \textstyle\sum_{i=1}^{n} \langle \mathbf{u}_i, \mathbf{y}_i \rangle, \mathsf{KeyGen}_3(\mathbf{y}_i) \end{aligned}$$

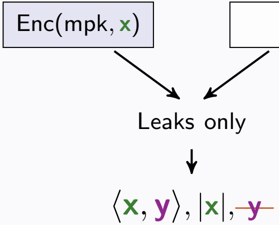
Our Construction Without Pairings

Pairing-free construction

- removed bilinear groups
- adaptive security
- support larger messages
- efficient schemes (linearly-sized ciphertexts and decryption keys)
- instantiations from DDH, LWE or DCR.
- polynomial number of slots

Function-Hiding Scheme

Security goal

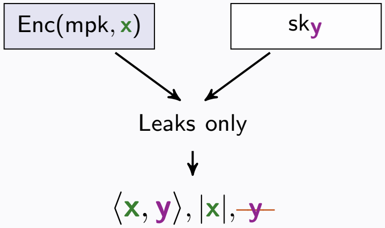


New multi-input function-hiding scheme for the inner product ✓

- Adaptively secure
- poly-many inputs

Function-Hiding Scheme

Security goal



New multi-input function-hiding scheme for the inner product ✓

- Adaptively secure
- poly-many inputs

Multi-input inner-product	Number of inputs	Assumptions
[AGRW17]	poly inputs	Pairing Groups
[DOT18] FH	unbounded poly inputs	Pairing Groups
This work FH	poly inputs	Pairing Groups

FH - function hiding

Future Work

Adapt our techniques for other classes of functions?

Thank you!

References

[ABDP15] Michel Abdalla, Florian Bourse, Angelo De Caro, and David Pointcheval. Simple functional encryption schemes for inner products. In Jonathan Katz, editor, *PKC 2015*, volume 9020 of *LNCS*, pages 733–751. Springer, Heidelberg, March / April 2015.

[AGRW17] Michel Abdalla, Romain Gay, Mariana Raykova, and Hoeteck Wee. Multi-input inner-product functional encryption from pairings. In Jean-Sébastien Coron and Jesper Buus Nielsen, editors, *EUROCRYPT 2017, Part I*, volume 10210 of *LNCS*, pages 601–626. Springer, Heidelberg, May 2017.

[AJ15] Prabhanjan Ananth and Abhishek Jain. Indistinguishability obfuscation from compact functional encryption. In Rosario Gennaro and Matthew J. B. Robshaw, editors, *CRYPTO 2015, Part I*, volume 9215 of *LNCS*, pages 308–326. Springer, Heidelberg, August 2015.

[ALS16] Shweta Agrawal, Benoît Libert, and Damien Stehlé. Fully secure functional encryption for inner products, from standard assumptions. In Matthew Robshaw and Jonathan Katz, editors, *CRYPTO 2016, Part III*, volume 9816 of *LNCS*, pages 333–362. Springer, Heidelberg, August 2016.

[BGJS15] Saikrishna Badrinarayanan, Divya Gupta, Abhishek Jain, and Amit Sahai. Multi-input functional encryption for unbounded arity functions. In Tetsu Iwata and Jung Hee Cheon, editors, *ASIACRYPT 2015, Part I*, volume 9452 of *LNCS*, pages 27–51. Springer, Heidelberg, November / December 2015.

[BKS16] Zvika Brakerski, Ilan Komargodski, and Gil Segev. Multi-input functional encryption in the private-key setting: Stronger security from weaker assumptions. In Marc Fischlin and Jean-Sébastien Coron, editors, *EUROCRYPT 2016, Part II*, volume 9666 of *LNCS*, pages 852–880. Springer, Heidelberg, May 2016.

[BLR+15] Dan Boneh, Kevin Lewi, Mariana Raykova, Amit Sahai, Mark Zhandry, and Joe Zimmerman. Semantically secure order-revealing encryption: Multi-input functional encryption without obfuscation. In Elisabeth Oswald and Marc Fischlin, editors, *EUROCRYPT 2015, Part II*, volume 9057 of *LNCS*, pages 563–594. Springer, Heidelberg, April 2015.

[BSW11] Dan Boneh, Amit Sahai, and Brent Waters. Functional encryption: Definitions and challenges. In Yuval Ishai, editor, *TCC 2011*, volume 6597 of *LNCS*, pages 253–273. Springer, Heidelberg, March 2011.

[DH76] Whitfield Diffie and Martin E. Hellman. New directions in cryptography. *IEEE Transactions on Information Theory*, 22(6):644–654, 1976.

[DOT18] Pratish Datta, Tatsuaki Okamoto, and Junichi Tomida. Full-hiding (unbounded) multi-input inner product functional encryption from the *k*-linear assumption. Cryptology ePrint Archive, Report 2018/061, 2018. `https://eprint.iacr.org/2018/061`.

[GGG+14] Shafi Goldwasser, S. Dov Gordon, Vipul Goyal, Abhishek Jain, Jonathan Katz, Feng-Hao Liu, Amit Sahai, Elaine Shi, and Hong-Sheng Zhou. Multi-input functional encryption. In Phong Q. Nguyen and Elisabeth Oswald, editors, *EUROCRYPT 2014*, volume 8441 of *LNCS*, pages 578–602. Springer, Heidelberg, May 2014.

[O'N10] Adam O'Neill. Definitional issues in functional encryption. Cryptology ePrint Archive, Report 2010/556, 2010. `http://eprint.iacr.org/2010/556`.