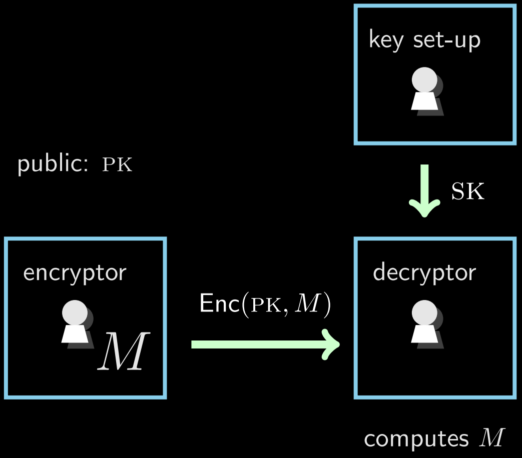
Functional Encryption with Bounded Collusions

Hoeteck Wee
George Washington University

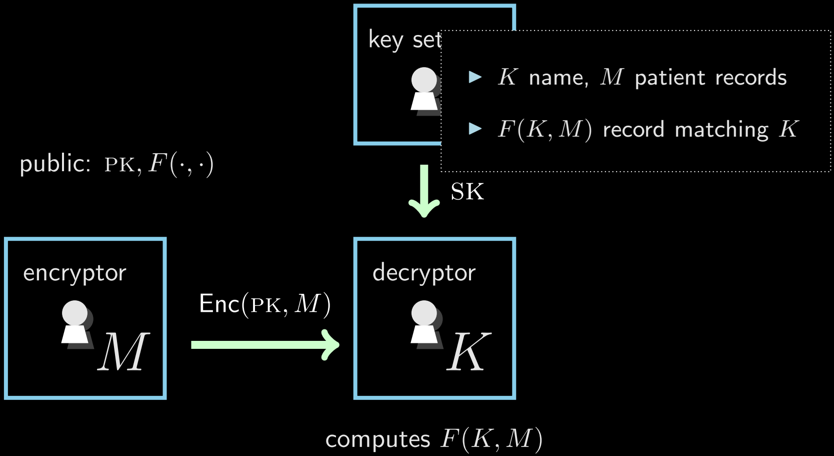
JOINT WORK WITH:

Serge Gorbunov & Vinod Vaikuntanathan
(University of Toronto)

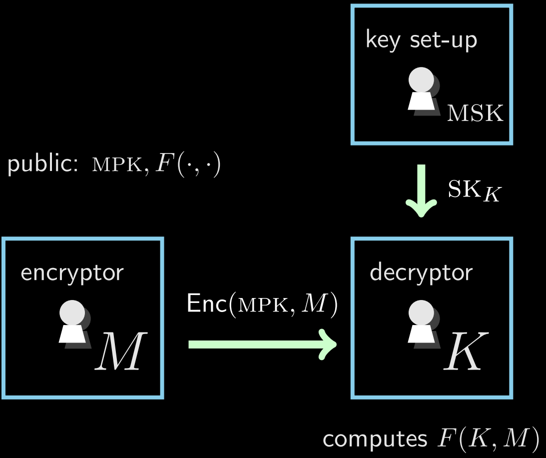
Public Key Encryption



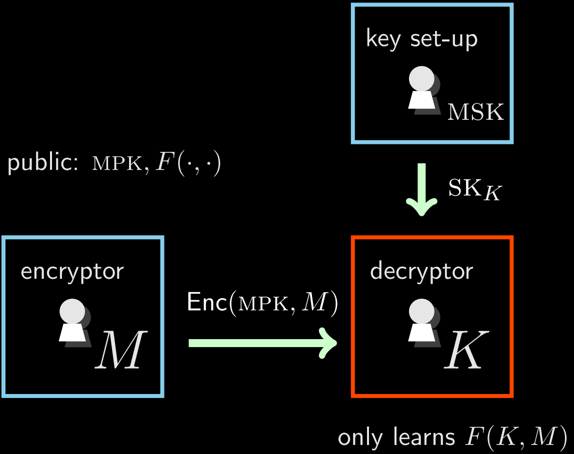
Functional Encryption



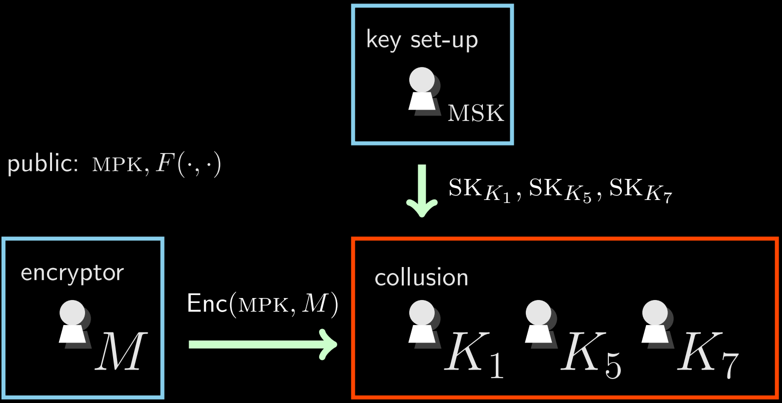
Functional Encryption



Functional Encryption



Functional Encryption

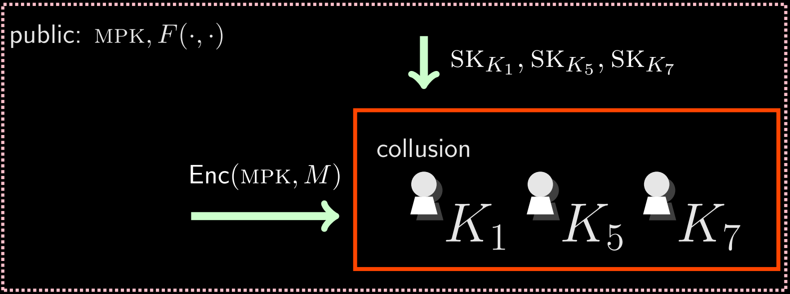


only learns $F(K_1, M), F(K_5, M), F(K_7, M)$

Functional Encryption

$$\text{simulator}\ \big(K_1, K_5, K_7, F(K_1, M), F(K_5, M), F(K_7, M)\ \big)$$

$$\approx$$

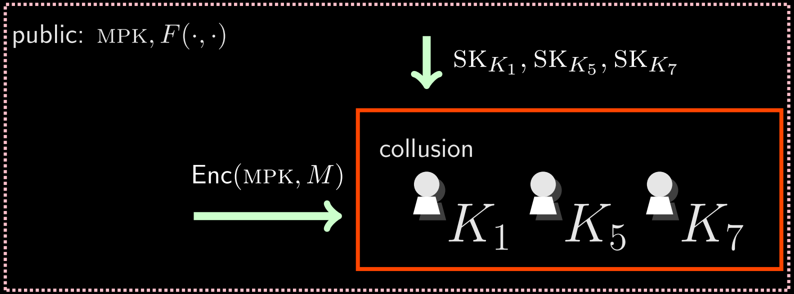


[Boneh Sahai Waters 11, O'Neill 11]

Functional Encryption

simulator $\left(K_1, K_5, K_7, F(K_1, M), F(K_5, M), F(K_7, M)\ \right)$

$$\approx$$



SIM security $\Rightarrow$ IND security, one-msg IND $\Rightarrow$ many-msg IND

Functional Encryption

- Predicate encryption $P(\cdot, \cdot)$ (public index)

$$F(K, w \| m) = \begin{cases} (w, m) & \text{if } P(K, w) = 1 \\ (w, \perp) & \text{otherwise} \end{cases}$$

Functional Encryption

- Predicate encryption $P(\cdot, \cdot)$ (public index)

$$F(K, w \| m) = \begin{cases} (w, m) & \text{if } P(K, w) = 1 \\ (w, \perp) & \text{otherwise} \end{cases}$$

Identity-based (IBE) [S84, BF01, C01]	$K \stackrel{?}{=} w$
Attribute-based (ABE) [GPSW06]	$K(w) \stackrel{?}{=} 1$, formula K
Inner product (IPE) [KSW08]	$\langle K, w \rangle \stackrel{?}{=} 0$

Q Can we construct Functional Encryption for all functions?

Q Can we construct Functional Encryption for all functions?

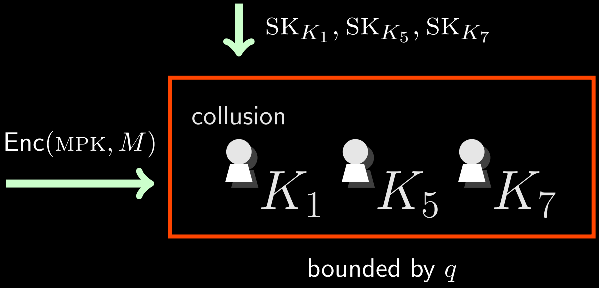
“ Yes, we can! ”

Q Can we construct Functional Encryption for all functions? (with bounded collusions)

“Yes, we can! ... with a small catch”

Q Can we construct Functional Encryption for all functions? (with bounded collusions)

"Yes, we can! ... with a small catch"



Q Can we construct Functional Encryption for all functions? (with bounded collusions)

“ Yes, we can! ... with a small catch ”

note. unbounded collusions impossible

[Agrawal Gorbunov Vaikuntanathan W 12]

Q Can we construct Functional Encryption for all functions? (with bounded collusions)

THIS WORK.

- poly-size circuits $\Longleftarrow$ IND-CPA PKE + small depth PRG
- predicate encryption $\Longleftarrow$ IND-CPA PKE

... for $q = \text{poly}(\cdot)$

Q Can we construct Functional Encryption for all functions? (with bounded collusions)

THIS WORK.

- poly-size circuits $\Longleftarrow$ IND-CPA PKE + small depth PRG
- predicate encryption $\Longleftarrow$ IND-CPA PKE

PREVIOUS WORK.

- IBE, $q = \mathrm{poly}(\cdot)$ [Dodis Katz Xu Yung 02, Goldwasser Lewko Wilson 12]
- poly-size circuits, $q = 1$ [Sahai Seyalioglu 10, Yao 86]

$\Longleftarrow$ IND-CPA PKE

Overview of Our Construction

$q = 1$, poly-size circuits

- based on Yao's garbled circuits
- can learn all input labels (thus M) with two queries

Overview of Our Construction

$q = 1$, poly-size circuits

↓

$+$ MPC [Ben-Or Goldwasser Wigderson 88]

c.f. [Ishai Kushilevitz Ostrovsky Sahai 07]

$q = \mathrm{poly}(\cdot)$, degree 3 polynomials

Overview of Our Construction

$q = 1$, poly-size circuits

↓ + MPC [Ben-Or Goldwasser Wigderson 88]

c.f. [Ishai Kushilevitz Ostrovsky Sahai 07]

$q = \text{poly}(\cdot)$, degree 3 polynomials

↓ + randomized encodings + small depth PRG

[Applebaum Ishai Kushilevitz 05]

$q = \text{poly}(\cdot)$, poly-size circuits

Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials

$q = 1$, poly-size circuits

↓ $+$ MPC [Ben-Or Goldwasser Wigderson 88]

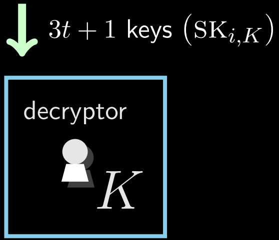
c.f. [Ishai Kushilevitz Ostrovsky Sahai 07]

$q = \mathrm{poly}(\cdot)$, degree 3 polynomials

i.e., $F(K, \cdot)$ is degree 3 (multivariate) for all K

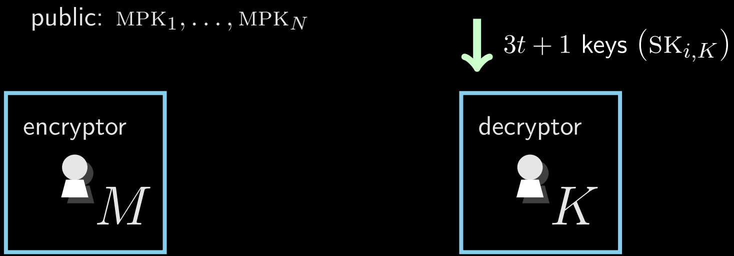
Construction for $q = \text{poly}(\cdot)$, Degree 3 Polynomials

public: $\text{MPK}_1, \ldots, \text{MPK}_N$



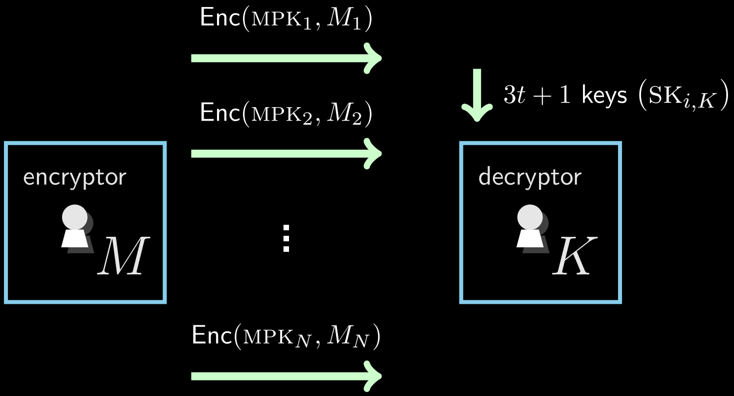
1. generate N copies of $q = 1$ scheme for $F_{\text{ONE}} := F$
2. decryptor gets random subset of $3t + 1$ secret keys

Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials

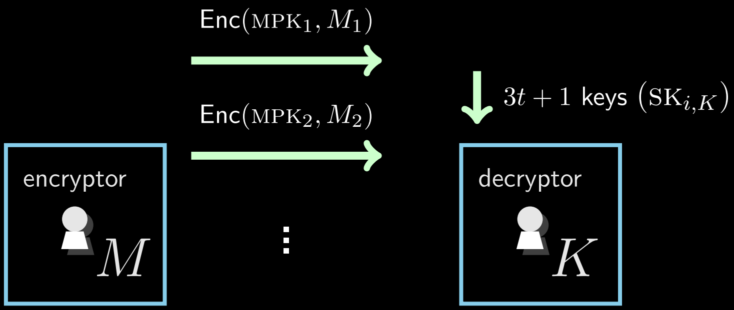


1. t-out-of-N secret share $M \to (M_1, \ldots, M_N)$ (ala [BGW 88])
2. encrypt the shares

Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials

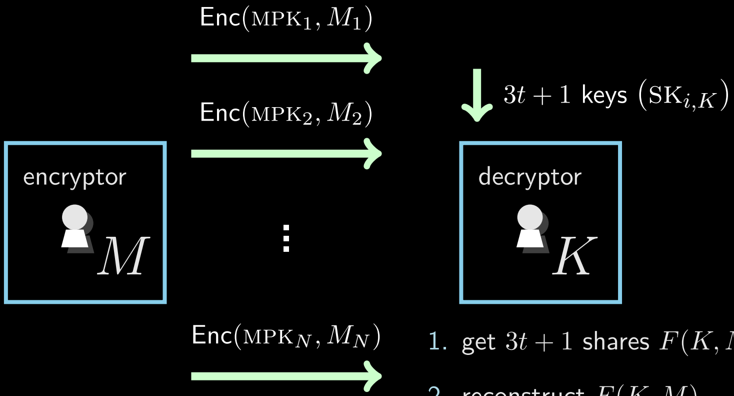


Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials



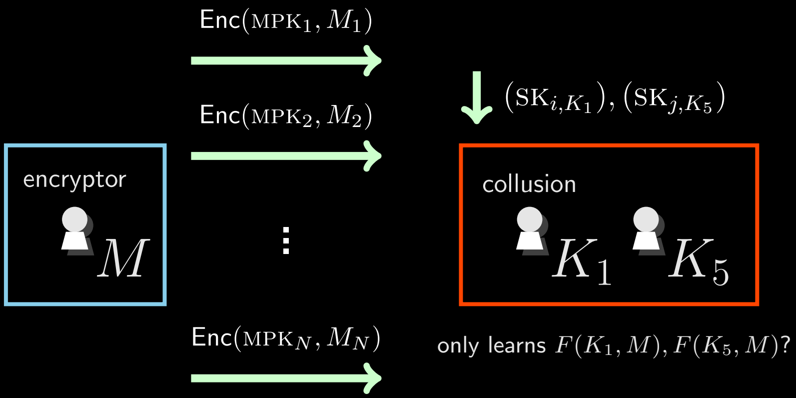
1. get $3t+1$ shares $F(K, M_i)$
   (shares lie on deg $3t$ poly)

Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials



1. get $3t+1$ shares $F(K, M_i)$
2. reconstruct $F(K, M)$

Construction for $q = \mathrm{poly}(\cdot)$, Degree 3 Polynomials



q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— okay if this happens at most t times (due to secret sharing)

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

issue 2. shares $\{F(K, M_i)\}$ of $F(K, M)$ not random

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

issue 2. shares $\{F(K, M_i)\}$ of $F(K, M)$ not random

— randomize by adding random shares $\{\sigma_i\}$ of 0

— $F_{\text{ONE}}(K, M_i \| \sigma_i) := F(K, M_i) + \sigma_i$

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

issue 2. shares $\{F(K, M_i)\}$ of $F(K, M)$ not random

— randomize by adding random shares $\{\sigma_i\}$ of 0

— $F_{\text{ONE}}(K, M_i \| \sigma_i) := F(K, M_i) + \sigma_i$

issue 3. correlation amongst shares of $F(K_1, M), F(K_5, M), \ldots$

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

issue 2. shares $\{F(K, M_i)\}$ of $F(K, M)$ not random

— randomize by adding random shares $\{\sigma_i\}$ of 0

— $F_{\text{ONE}}(K, M_i \| \sigma_i) := F(K, M_i) + \sigma_i$

issue 3. correlation amongst shares of $F(K_1, M), F(K_5, M), \ldots$

— refresh using q-wise independent random shares of 0

q-FE for Degree 3 Polynomials

issue 1. adversary gets two secret keys for MPK_i, learns M_i

— use family of sets with small pairwise intersection (at most t)

issue 2. shares $\{F(K, M_i)\}$ of $F(K, M)$ not random

— randomize by adding random shares $\{\sigma_i\}$ of 0

— $F_{\mathrm{ONE}}(K, M_i \| \sigma_i) := F(K, M_i) + \sigma_i$

issue 3. correlation amongst shares of $F(K_1, M), F(K_5, M), \ldots$

— $F_{\mathrm{ONE}}(K \| \Delta, M_i \| \vec{\sigma}_i) := F(K, M_i) + \sum_{a \in \Delta} \vec{\sigma}_i[a]$

— Δ : family of cover-free sets

Conclusion

THIS WORK. Functional Encryption with bounded collusion

- feasibilty result via MPC
- poly-size circuits $\Longleftarrow$ IND-CPA PKE + 'small depth' PRG
- predicate encryption $\Longleftarrow$ IND-CPA PKE

Conclusion

THIS WORK. Functional Encryption with bounded collusion

- feasibilty result via MPC
- poly-size circuits $\Longleftarrow$ IND-CPA PKE + ‘small depth’ PRG
- predicate encryption $\Longleftarrow$ IND-CPA PKE

NEXT?

- IND-based functional encryption with unbounded collusion
- further connections between MPC and functional encryption?

终

THE END