RSAConference2019

San Francisco | March 4 – 8 | Moscone Center

BETTER.

SESSION ID: CRYP-T09

Efficient Function-Hiding Functional Encryption: From Inner-Products to Orthogonality

Authors:

Manuel Barbosa, Dario Catalano, Azam Soleimanian, and Bogdan Warinschi

Corresponding author :Azam.Soleimanian@ens.fr

Motivations: Functional Encryption for Orthogonality (OFE)

- Privacy-preserving role-based access control
- Keyword search over encrypted data

r_f

r_u

$\underbrace{\quad r_f \qquad\qquad\qquad r_u \quad}$

Access iff $< r_f, r_u > \neq 0$

where $< r_f, r_u > = \sigma \; r_f^i r_u^i$

No information about r_f or $< r_f, r_u >$ when $< r_f, r_u > \neq 0$

RSA Conference 2019

Functional Encryption for Orthogonality

Functional Encryption (for $F: X \times Y \longrightarrow Z$)

$Setup(1^{\lambda}) \longrightarrow (msk, mpk)$

$Enc(mpk, x) \longrightarrow ct$

$KeyGen(msk, y) \longrightarrow sk$

$Dec(ct, sk)$

Inner-Product (IPFE)

$$F(x,y) = \langle x, y \rangle = \Sigma_{i=1}^{n} x_i y_i$$

$r \cdot < X, Y >$

$$F(x,y) = \begin{cases} 1 & \langle x, y \rangle = 0 \\ 0 & othw \end{cases}$$

Orthogonality (OFE)

From IPFE to OFE

Randomization + function-hiding

IPFE → OFE

Algorithm (FH-OFE from FH-IPFE)

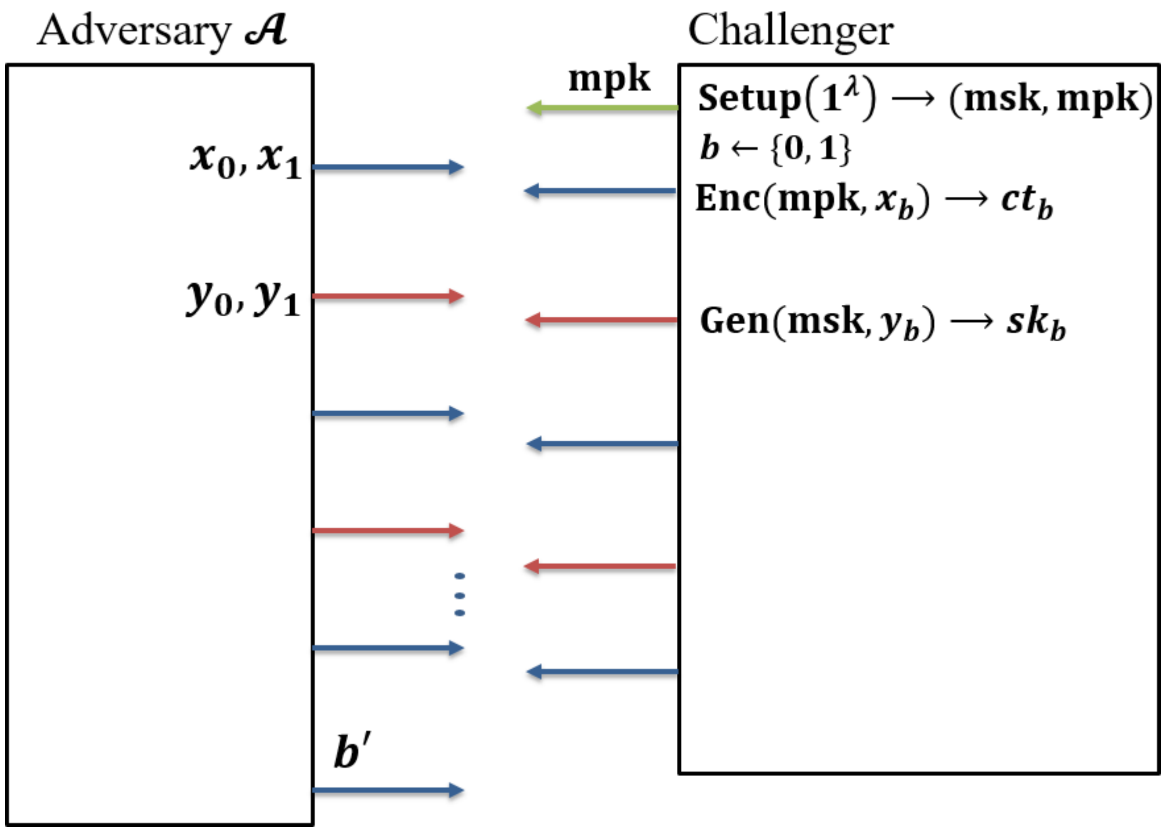
$\mathsf{FE}^*.\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})$	$\mathsf{FE}^*.\mathsf{Enc}(\mathsf{msk}, \mathbf{x})$	$\mathsf{FE}^*.\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}_y)$
$r_y \leftarrow \mathbb{Z}_q$	$\mathsf{ct} \leftarrow \mathsf{FE}.\mathsf{Enc}(\mathsf{msk}, \mathbf{x})$	$v \leftarrow \mathsf{FE}.\mathsf{Dec}(\mathsf{ct}, \mathsf{sk})$
$\boxed{\mathbf{y}^* \leftarrow r_y \cdot \mathbf{y}}$	*Return* ct	*If* $v = 0$ *return* 1
$\mathsf{sk}_y \leftarrow \mathsf{FE}.\mathsf{KeyGen}(\mathsf{msk}, \boxed{\mathbf{y}^*})$		*Else return* 0
Return sk_y		

FH-OFE

- no information about $\mathbf{x}$
- no information about $\mathbf{y}$
- no information about $< \mathbf{x}, \mathbf{y} >$ when $< \mathrm{x}, \mathrm{y} > \neq 0$

Security notion in FH-FE

- Selective: Ask all the challenges at the beginning
- Adaptive: Ask whenever you want



One vs. Many

Selective vs. Adaptive

Coming back to the construction

Algorithm (FH-OFE from FH-IPFE)

$\underline{\mathsf{FE}^*.\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y})}$

$r_y \leftarrow \mathbb{Z}_q$

$\boxed{\mathbf{y}^* \leftarrow r_y \cdot \mathbf{y}}$

$\mathsf{sk}_y \leftarrow \mathsf{FE}.\mathsf{KeyGen}(\mathsf{msk}, \boxed{\mathbf{y}^*})$

Return sk_y

$\underline{\mathsf{FE}^*.\mathsf{Enc}(\mathsf{msk}, \mathbf{x})}$

$\mathsf{ct} \leftarrow \mathsf{FE}.\mathsf{Enc}(\mathsf{msk}, \mathbf{x})$

Return ct

$\underline{\mathsf{FE}^*.\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}_y)}$

$v \leftarrow \mathsf{FE}.\mathsf{Dec}(\mathsf{ct}, \mathsf{sk})$

If $v = 0$ *return* 1

Else return 0

Security level: one-selective

RSAConference2019

Going to Many-Adaptive security

FH-OFE in Generic Group Model

FH-OFE in generic group model (GGM)

- Group Operations in GGM
  - Encoding
  - Add
  - Pair
  - Zero-test
- Pros and Cons with GGM?
  - Oracle access to group operations
  - non-generic attacks can be inefficient
  - Flexibility to present efficient constructions
  - Preventing many-ciphertext attacks

FH-OFE in GGM

❖ FH-IPFE by Kim et al. SCN 2018

Algorithm (FH-OFE in GGM)

- $\mathsf{Setup}(1^\lambda) \rightarrow \mathsf{msk}$
  where $(\mathbf{B}, \mathbf{B}^*)$, $\mathbf{B} \leftarrow \mathbb{Z}^{n\times n}$, *and* $\mathbf{B}^* = \det(\mathbf{B}) \cdot (B^{-1})^T$
- $\mathsf{Enc}(\mathsf{msk}, \mathbf{x}) \rightarrow \mathsf{ct}$ *where* $\mathsf{ct} = [\boxed{\beta} \cdot \mathbf{x} \cdot {}^T \mathbf{B}^*]_2$
- $\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y}) \rightarrow sk_y$ *where* $\mathsf{sk}_y = [\boxed{\alpha} \cdot \mathbf{y}^T \cdot \mathbf{B}]_1$
- $\mathsf{Dec}(\mathsf{ct}, \mathsf{sk}) \rightarrow \prod_{i=1}^{n} e(sk[i], ct[i])$

Security Level: many-Adaptive

RSAConference2019

FH-OFE in Standard Model

FH-OFE in standard model (SM)

❖ FH-IPFE by Lin CRYPTO 2017

$$\mathrm{KeyGen}(\ \mathrm{Enc}_{\mathrm{mpk}}(\boxed{\mathbf{x}})\ )$$

$$\mathrm{Enc}(\ \boxed{\mathrm{KeyGen}_{\mathrm{msk}}(\mathbf{y})}\ )$$

- General Construction by Lin
  - Requirements on the underlying scheme
  - Adding multi-linearity
  - Selective results in selective
  - Instantiation: scheme of Abdalla et al. PKC 2015

FH-OFE in standard model (SM)

Algorithm (FH-OFE in SM)

- $\mathsf{Setup}(1^\lambda, 1^n)$:

  $(\mathsf{msk}_1, \mathsf{mpk}_1) \leftarrow \Gamma_1.\mathsf{Setup}(1^\lambda, 1^n)$ *and*
  $(\mathsf{msk}_2, \mathsf{mpk}_2) \leftarrow \Gamma_2.\mathsf{Setup}(1^\lambda, 1^{n+1})$.
  output $k = (\mathsf{msk}; \mathsf{mpk}) = (\mathsf{msk}_1, \mathsf{msk}_2; \mathsf{mpk}_1, \mathsf{mpk}_2)$

- $\mathsf{Enc}(k, \mathbf{x})$:

  $[\mathsf{ct}]_1 = \Gamma_1.\mathsf{Enc}(\mathsf{mpk}_1, \mathbf{x})$ *where* $\mathbf{x} \in \mathbb{Z}^n$, *set*
  $[\mathsf{wCT}]_1 = \Gamma_2.\mathsf{KeyGen}(\mathsf{msk}_2, \boxed{\mathsf{ct}})$

- $\mathsf{KeyGen}(k, \mathbf{y})$:

  $[\mathsf{sk}]_2 = \Gamma_1.\mathsf{KeyGen}(\mathsf{msk}_1, \mathbf{y})$ *where* $\mathbf{y} \in \mathbb{Z}^n$, *set*
  $[\mathsf{wSK}]_2 = \Gamma_2.\mathsf{Enc}(\mathsf{mpk}_2, \boxed{\mathsf{sk}})$

- $\mathsf{Dec}(\mathsf{wSK}, \mathsf{wCT})$: $\Gamma_2.\mathsf{Dec}([\mathsf{wSK}]_2, [\mathsf{wCT}]_1)$

Security level: Depends on the underlying scheme

Instantiation: Wee's Scheme TCC 2017

Algorithm

$\underline{\mathsf{Setup}(1^\lambda):}$ $\mathbf{A} \leftarrow \mathbb{Z}^{k+1\times k}$ *For* $i \in [n]$: $\quad \mathbf{W}_i \leftarrow \mathbb{Z}^{k+1\times k+1}$ $\mathsf{msk} \leftarrow (\mathbf{A}, \{\mathbf{W}_i\}_{i=1}^n)$ $\mathsf{mpk} \leftarrow ([\mathbf{A}^\top]_1, \{[\mathbf{A}^\top \mathbf{W}_i]_1\}_{i=1}^n)$ *Return* $(\mathsf{msk}, \mathsf{mpk})$	$\underline{\mathsf{Enc}(\mathsf{mpk}, \mathbf{x}):}$ $\mathbf{s} \leftarrow \mathbb{Z}^k$ $\mathbf{U} \leftarrow \mathbb{Z}^{k+1\times k+1}$ $\mathbf{M}_0 \leftarrow \mathbf{s}^\top \mathbf{A}^\top$ $\mathsf{ct} \leftarrow [\mathbf{M}_0 \| \{\mathbf{M}_0(\mathbf{x}_i\mathbf{U} + \mathbf{W}_i)\}_{i=1}^n]_1$ *Return* ct
$\underline{\mathsf{KeyGen}(\mathsf{msk}, \mathbf{y}):}$ $\mathbf{r} \leftarrow \mathbb{Z}^{k+1}$ $\mathsf{sk} \leftarrow [-\sum_{i=0}^n \mathbf{y}_i \mathbf{W}_i \mathbf{r} \| \{\mathbf{y}_i \mathbf{r}\}_{i=1}^n]_2$ *Return* sk	$\underline{\mathsf{Dec}(\mathsf{sk}, \mathsf{ct}):}$ *Return* $\langle \mathsf{ct}, \mathsf{sk} \rangle = \mathbf{1}$

- Instantiation: Harder but possible
  - Matrix scales
  - MDDH assumption
  - Many-Selective secure

From Selective to Adaptive in SM

Complexity Leveraging (CL)

- Converting selective security to adaptive security
- Losing a factor of security (is it tolerable?)

- CL on the general construction
  - Security loss: q^{τ} where $\tau = 2n(\boxed{q_e + q_k})$ Not tolerable, So?
- CL on underlying schemes?
  - Security loss: q^{2n} Tolerable if n is small enough

One-SEL OFE $\xrightarrow{\text{CL}}$ One-AD OFE $\xrightarrow{\text{Hybrid}}$ Many-AD OFE $\xrightarrow{\text{Lin's}}$ Many-AD FH-OFE

Implementation

Timing values in milliseconds

	GGM			SM		
N	Extract	Encrypt	Decrypt	Extract	Encrypt	Decrypt
16	6	2	10	36	15	60
32	12	4	19	71	28	116
64	22	9	37	139	60	231
128	46	20	73	270	112	463
256	100	44	155	558	229	968

Lengths in Kilobytes

	GGM		SM	
N	Keys	Cph	Keys	Cph
16	0,99	0,50	6,34	3,18
32	1,99	1,00	12,30	6,16
64	3,98	1,99	24,23	12,14
128	7,95	3,98	48,09	24,09
256	15,91	7,97	95,81	48,00

Implementation

- MacBook Pro, 2.9 GHz Intel Core i5, RAM 16 GB
- C++
  - SCIPR Lab's library for finite fields and elliptic curves (libff)
    - Curve: BN128 (BN254)
  - Shoup's Number Theory Library (NTL)
  - GNU Multiprecision Library (GMP)

www.shoup.net/ntl/
www.gmplib.org
www.github.com/scipr-lab/libff
www.github.com/zcash/zcash/issues/2502

Comparison

Scheme	GGM	SM	Shen et al.	Kawai et al.
security	full	full*	selective	full
group order	prime	prime	composite	prime
assumption	GGM	MDDH, DDH	C3DH, DLIN	DLIN
key size	n	$6n+6$	$4n+4$	$6n$
ciphertext size	n	$6n+6$	$4n+4$	$6n$
key extraction	n	$12n+9$	$32n+4$	$6n$
encryption	n	$12n+9$	$24n+16$	$6n$
decryption	n	$6n+6$	$4n+4$	$6n$

Applications

- Privacy-preserving subset relation
  - Sorting algorithm
  - Searchable encryption
- Range queries
- Access Control

$$B \subseteq A$$

$$\mathsf{mRep}(A) := \begin{cases} \boldsymbol{x}_i = 1 & \text{if } u_i \in A, 1 \leq i \leq n \\ \boldsymbol{x}_i = 0 & \text{if } u_i \notin A, 1 \leq i \leq n \\ \boldsymbol{x}_{n+1} = -1 & \end{cases}$$

$$\mathsf{kRep}(B) := \begin{cases} \boldsymbol{y}_i = 1 & \text{if } u_i \in B, 1 \leq i \leq n \\ \boldsymbol{y}_i = 0 & \text{if } u_i \notin B, 1 \leq i \leq n \\ \boldsymbol{y}_{n+1} = |B| & \end{cases}$$

$$B \subseteq A \quad \text{iff} \quad < \mathrm{mRep}(A), \mathrm{kRep}(B) > = 0$$

References

- Abdalla, M., Bourse, F., Caro, A.D., Pointcheval, D.: Simple functional encryption schemes for inner products. Public-Key Cryptography - PKC 2015.
- Kawai, Y., Takashima, K.: Predicate- and attribute-hiding inner product encryption in a public key setting. Pairing 2013, Revised
- Kim, S., Lewi, K., Mandal, A., Montgomery, H.W., Roy, A., Wu, D.J.: Function hiding inner product encryption is practical. SCN 2018
- Lin, H.: Indistinguishability obfuscation from SXDH on 5-linear maps and locality-5 prgs. Advances in Cryptology - CRYPTO 2017.
- Shen, E., Shi, E., Waters, B.: Predicate privacy in encryption systems. Theory of Cryptography - TCC 2009. Proceedings, pp. 457–473 (2009)
- Wee, H.: Attribute-hiding predicate encryption in bilinear groups, revisited. TCC 2017.

RSAConference2019

Summery:

- Functional encryption for orthogonality
- Function-hiding property
- IPFE + Randomization + function hiding ⟶ one-selective FH-OFE
- FH-OFE in GGM with many-adaptive security is possible
- Wee’s OFE + Lin’s Transformation ⟶ many-selective-secure FH-OFE
- CL on Wee’s OFE+ hybrid +Lin’s transformation⟶many-adaptive-secure FH-OFE
- FH-OFE ⟶privacy-preserving subset relation

Thanks