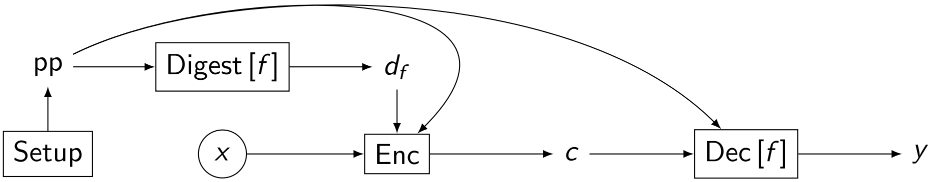
Lattice-based Laconic Function Evaluation (LFE)

Yi Tang

October 10, 2024

Definition of LFE

Syntax [QWW18]:

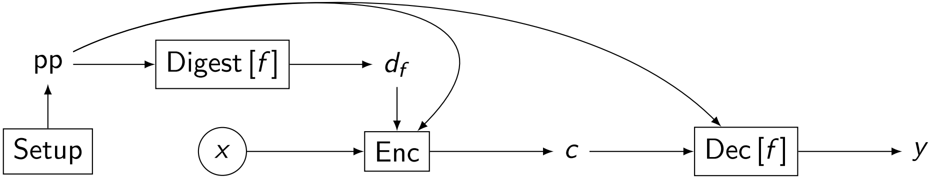


Properties:

- Correctness: $y = f(x)$.
- Security: $\mathrm{Enc}(\mathrm{pp}, d_f, x) \overset{c}{\approx} \mathcal{S}(\mathrm{pp}, f, d_f, f(x))$; adaptive: f, x chosen by $\mathcal{A}(\mathrm{pp})$.
- Efficiency: *laconic*, $|\mathrm{pp}|, |d_f| \ll |f|$.

Definition of LFE

Syntax [QWW18]:

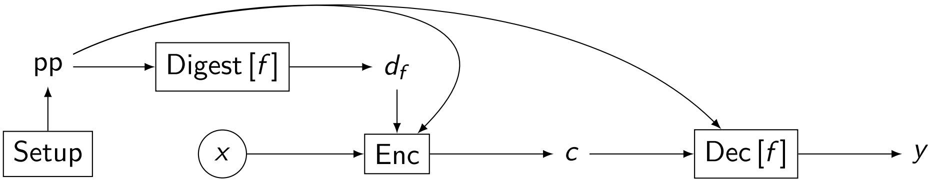


Properties:

- Correctness: $y = f(x)$.
- Security: $\mathrm{Enc}(\mathrm{pp}, d_f, x) \stackrel{c}{\approx} \mathcal{S}(\mathrm{pp}, f, d_f, f(x))$; adaptive: f, x chosen by $\mathcal{A}(\mathrm{pp})$.
- Efficiency: *laconic*, $|\mathrm{pp}|, |d_f| \ll |f|$.

Definition of LFE

Syntax [QWW18]:

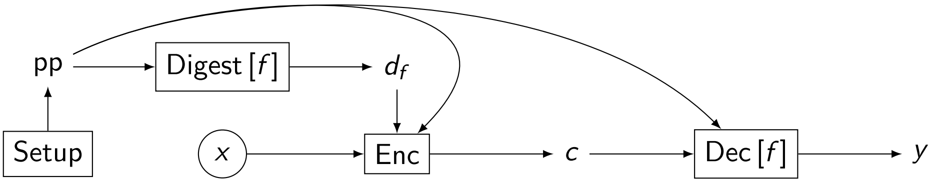


Properties:

- Correctness: $y = f(x)$.
- Security: $\mathrm{Enc}(\mathrm{pp}, d_f, x) \overset{c}{\approx} \mathcal{S}(\mathrm{pp}, f, d_f, f(x))$; adaptive: f, x chosen by $\mathcal{A}(\mathrm{pp})$.
- Efficiency: *laconic*, $|\mathrm{pp}|, |d_f| \ll |f|$.

Definition of LFE

Syntax [QWW18]:



Properties:

- Correctness: $y = f(x)$.
- Security: $\mathsf{Enc}(\mathsf{pp}, d_f, x) \overset{c}{\approx} \mathcal{S}(\mathsf{pp}, f, d_f, f(x))$; adaptive: f, x chosen by $\mathcal{A}(\mathsf{pp})$.
- Efficiency: *laconic*, $|\mathsf{pp}|, |d_f| \ll |f|$.

Applications of LFE

Motivation: $f = f_D$ for a large dataset D.

Applications:

- "Bob-optimized" 2-round 2PC. (Cf., FHE solution is "Alice-optimized".)
- "Online-optimized" MPC.
- (Alternative construction of) succinct (1-key) *functional encryption* (FE), then *reusable garbled circuit* by [GKP+13].

Applications of LFE

Motivation: $f = f_D$ for a large dataset D.

Applications:

- "Bob-optimized" 2-round 2PC. (Cf., FHE solution is "Alice-optimized".)
- "Online-optimized" MPC.
- (Alternative construction of) succinct (1-key) *functional encryption* (FE), then *reusable garbled circuit* by [GKP+13].

Applications of LFE

Motivation: $f = f_D$ for a large dataset D.

Applications:

- "Bob-optimized" 2-round 2PC. (Cf., FHE solution is "Alice-optimized".)
- "Online-optimized" MPC.
- (Alternative construction of) succinct (1-key) *functional encryption* (FE), then *reusable garbled circuit* by [GKP+13].

Applications of LFE

Motivation: $f = f_D$ for a large dataset D.

Applications:

- "Bob-optimized" 2-round 2PC. (Cf., FHE solution is "Alice-optimized".)
- "Online-optimized" MPC.
- (Alternative construction of) succinct (1-key) *functional encryption* (FE), then *reusable garbled circuit* by [GKP+13].

Recap 1/3: Learning with Errors (LWE)

LWE:

- Take $\mathbf{A} \leftarrow \mathbb{Z}_q^{n\times m}, \mathbf{s} \leftarrow \mathbb{Z}_q^n$, and sufficiently large noise $\mathbf{e}$.
- Then $(\mathbf{A}; \mathbf{s}^\top\mathbf{A} + \mathbf{e}^\top) \overset{c}{\approx} (\mathbf{A}; U)$, by hardness of lattice problems (e.g. SVP).

Recap 2/3: GSW FHE

Gadget $\mathbf{g} := (1, 2, \ldots, 2^{\ell-1})$, $\mathbf{G}_n := \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{n \times n\ell}$, $\ell = \lceil \log_2 q \rceil$.

GSW FHE [GSW13]:

- Secret key $k = \mathbf{s} = (-\bar{\mathbf{s}}; 1)$.
- By LWE, sample $\mathbf{A} = (\bar{\mathbf{A}}; \bar{\mathbf{s}}^\top \bar{\mathbf{A}} + \mathbf{e}^\top)$ satisfies $\mathbf{A} \overset{c}{\approx} U$ and $\mathbf{s}^\top \mathbf{A} = \mathbf{e}^\top \approx \mathbf{0}^\top$.
- $\mathsf{Enc}(k = \mathbf{s}, x \in \{0, 1\})$: $\mathbf{C} = \mathbf{A} + x \cdot \mathbf{G}$.
  (For bit string (row vector) x, $\mathbf{C} = \mathbf{A} + x \otimes \mathbf{G}$.)
- $\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$;
  $\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$.

Recap 2/3: GSW FHE

Gadget $\mathbf{g} := (1, 2, \ldots, 2^{\ell-1})$, $\mathbf{G}_n := \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{n \times n\ell}$, $\ell = \lceil \log_2 q \rceil$.

GSW FHE [GSW13]:

- Secret key $k = \mathbf{s} = (-\bar{\mathbf{s}}; 1)$.
- By LWE, sample $\mathbf{A} = (\bar{\mathbf{A}}; \bar{\mathbf{s}}^\top \bar{\mathbf{A}} + \mathbf{e}^\top)$ satisfies $\mathbf{A} \overset{c}{\approx} U$ and $\mathbf{s}^\top \mathbf{A} = \mathbf{e}^\top \approx \mathbf{0}^\top$.
- $\mathrm{Enc}(k = \mathbf{s}, x \in \{0, 1\})$: $\mathbf{C} = \mathbf{A} + x \cdot \mathbf{G}$.
  (For bit string (row vector) x, $\mathbf{C} = \mathbf{A} + x \otimes \mathbf{G}$.)
- $\mathrm{HEval}^{\mathrm{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$;
  $\mathrm{HEval}^{\mathrm{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$.

Recap 2/3: GSW FHE

Gadget $\mathbf{g} := (1, 2, \ldots, 2^{\ell-1})$, $\mathbf{G}_n := \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{n \times n\ell}$, $\ell = \lceil \log_2 q \rceil$.

GSW FHE [GSW13]:

- Secret key $k = \mathbf{s} = (-\bar{\mathbf{s}}; 1)$.
- By LWE, sample $\mathbf{A} = (\bar{\mathbf{A}}; \bar{\mathbf{s}}^\top \bar{\mathbf{A}} + \mathbf{e}^\top)$ satisfies $\mathbf{A} \overset{c}{\approx} U$ and $\mathbf{s}^\top \mathbf{A} = \mathbf{e}^\top \approx \mathbf{0}^\top$.
- $\mathsf{Enc}(k = \mathbf{s}, x \in \{0,1\})$: $\mathbf{C} = \mathbf{A} + x \cdot \mathbf{G}$.
  (For bit string (row vector) x, $\mathbf{C} = \mathbf{A} + x \otimes \mathbf{G}$.)
- $\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$;
  $\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$.

Recap 2/3: GSW FHE

Gadget $\mathbf{g} := (1, 2, \ldots, 2^{\ell-1})$, $\mathbf{G}_n := \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{n \times n\ell}$, $\ell = \lceil \log_2 q \rceil$.

GSW FHE [GSW13]:

- Secret key $k = \mathbf{s} = (-\bar{\mathbf{s}}; 1)$.
- By LWE, sample $\mathbf{A} = (\bar{\mathbf{A}}; \bar{\mathbf{s}}^\top \bar{\mathbf{A}} + \mathbf{e}^\top)$ satisfies $\mathbf{A} \overset{c}{\approx} U$ and $\mathbf{s}^\top \mathbf{A} = \mathbf{e}^\top \approx \mathbf{0}^\top$.
- $\mathsf{Enc}(k = \mathbf{s}, x \in \{0,1\})$: $\mathbf{C} = \mathbf{A} + x \cdot \mathbf{G}$.
  (For bit string (row vector) x, $\mathbf{C} = \mathbf{A} + x \otimes \mathbf{G}$.)
- $\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$;
  $\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$.

Recap 2/3: GSW FHE

Gadget $\mathbf{g} := (1, 2, \ldots, 2^{\ell-1})$, $\mathbf{G}_n := \mathbf{I}_n \otimes \mathbf{g} \in \mathbb{Z}_q^{n \times n\ell}$, $\ell = \lceil \log_2 q \rceil$.

GSW FHE [GSW13]:

- Secret key $k = \mathbf{s} = (-\bar{\mathbf{s}}; 1)$.
- By LWE, sample $\mathbf{A} = (\bar{\mathbf{A}}; \bar{\mathbf{s}}^\top \bar{\mathbf{A}} + \mathbf{e}^\top)$ satisfies $\mathbf{A} \overset{c}{\approx} U$ and $\mathbf{s}^\top \mathbf{A} = \mathbf{e}^\top \approx \mathbf{0}^\top$.
- $\mathsf{Enc}(k = \mathbf{s}, x \in \{0, 1\})$: $\mathbf{C} = \mathbf{A} + x \cdot \mathbf{G}$.
  (For bit string (row vector) x, $\mathbf{C} = \mathbf{A} + x \otimes \mathbf{G}$.)
- $\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$;
  $\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$.

Recap 3/3: GSW/BGGHNSVV Homomorphism

$$\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$$
$$\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$$

BGGHNSVV ABE's attribute encoding [BGG+14]:

- Take uniform $\mathbf{M}$ (cf. $\mathbf{C}$) and attribute encoding $\mathbf{A} = \mathbf{M} - x \otimes \mathbf{G}$.
- Same $\mathsf{HEval}^{\mathsf{pub}}$ over $\mathbf{M}$.
- $\mathsf{HEval}[+]((\mathbf{A}_1, \mathbf{A}_2), (-, -), (-, -)) = \mathbf{A}_1 + \mathbf{A}_2$,
  $\mathsf{HEval}[\times]((\mathbf{A}_1, \mathbf{A}_2), (-, \mathbf{M}_2), (x_1, -)) = \mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{M}_2) + x_1 \cdot \mathbf{A}_2$.
- S.t., $\mathsf{HEval}[f](\mathbf{A}, \mathbf{M}, x) = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) - f(x) \otimes \mathbf{G}$.

Recap 3/3: GSW/BGGHNSVV Homomorphism

$$\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$$

$$\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$$

BGGHNSVV ABE's attribute encoding [BGG+14]:

- Take uniform $\mathbf{M}$ (cf. $\mathbf{C}$) and attribute encoding $\mathbf{A} = \mathbf{M} - x \otimes \mathbf{G}$.
- Same $\mathsf{HEval}^{\mathsf{pub}}$ over $\mathbf{M}$.
- $\mathsf{HEval}[+]((\mathbf{A}_1, \mathbf{A}_2), (-, -), (-, -)) = \mathbf{A}_1 + \mathbf{A}_2$,
  $\mathsf{HEval}[\times]((\mathbf{A}_1, \mathbf{A}_2), (-, \mathbf{M}_2), (x_1, -)) = \mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{M}_2) + x_1 \cdot \mathbf{A}_2$.
- S.t., $\mathsf{HEval}[f](\mathbf{A}, \mathbf{M}, x) = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) - f(x) \otimes \mathbf{G}$.

Recap 3/3: GSW/BGGHNSVV Homomorphism

$$\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$$
$$\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$$

BGGHNSVV ABE's attribute encoding [BGG+14]:

- Take uniform $\mathbf{M}$ (cf. $\mathbf{C}$) and attribute encoding $\mathbf{A} = \mathbf{M} - x \otimes \mathbf{G}$.
- Same $\mathsf{HEval}^{\mathsf{pub}}$ over $\mathbf{M}$.
- $\mathsf{HEval}[+]((\mathbf{A}_1, \mathbf{A}_2), (-,-), (-,-)) = \mathbf{A}_1 + \mathbf{A}_2$,
  $\mathsf{HEval}[\times]((\mathbf{A}_1, \mathbf{A}_2), (-, \mathbf{M}_2), (x_1, -)) = \mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{M}_2) + x_1 \cdot \mathbf{A}_2$.
- S.t., $\mathsf{HEval}[f](\mathbf{A}, \mathbf{M}, x) = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) - f(x) \otimes \mathbf{G}$.

Recap 3/3: GSW/BGGHNSVV Homomorphism

$$\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$$
$$\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$$

BGGHNSVV ABE's attribute encoding [BGG+14]:

- Take uniform $\mathbf{M}$ (cf. $\mathbf{C}$) and attribute encoding $\mathbf{A} = \mathbf{M} - x \otimes \mathbf{G}$.
- Same $\mathsf{HEval}^{\mathsf{pub}}$ over $\mathbf{M}$.
- $\mathsf{HEval}[+]((\mathbf{A}_1, \mathbf{A}_2), (-,-), (-,-)) = \mathbf{A}_1 + \mathbf{A}_2$,
  $\mathsf{HEval}[\times]((\mathbf{A}_1, \mathbf{A}_2), (-, \mathbf{M}_2), (x_1, -)) = \mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{M}_2) + x_1 \cdot \mathbf{A}_2$.
- S.t., $\mathsf{HEval}[f](\mathbf{A}, \mathbf{M}, x) = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) - f(x) \otimes \mathbf{G}$.

Recap 3/3: GSW/BGGHNSVV Homomorphism

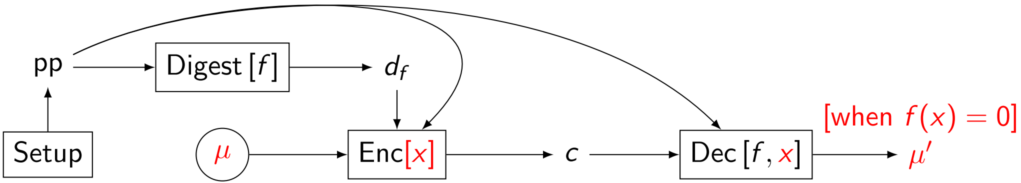
$$\mathsf{HEval}^{\mathsf{pub}}[+]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 + \mathbf{C}_2 = (\mathbf{A}_1 + \mathbf{A}_2) + (x_1 + x_2) \cdot \mathbf{G}$$
$$\mathsf{HEval}^{\mathsf{pub}}[\times]((\mathbf{C}_1, \mathbf{C}_2)) = \mathbf{C}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) = (\mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{C}_2) + x_1 \cdot \mathbf{A}_2) + (x_1 x_2) \cdot \mathbf{G}$$

BGGHNSVV ABE's attribute encoding [BGG+14]:

- Take uniform $\mathbf{M}$ (cf. $\mathbf{C}$) and attribute encoding $\mathbf{A} = \mathbf{M} - x \otimes \mathbf{G}$.
- Same $\mathsf{HEval}^{\mathsf{pub}}$ over $\mathbf{M}$.
- $\mathsf{HEval}[+]((\mathbf{A}_1, \mathbf{A}_2), (-,-), (-,-)) = \mathbf{A}_1 + \mathbf{A}_2$,
  $\mathsf{HEval}[\times]((\mathbf{A}_1, \mathbf{A}_2), (-, \mathbf{M}_2), (x_1, -)) = \mathbf{A}_1 \cdot \mathbf{G}^{-1}(\mathbf{M}_2) + x_1 \cdot \mathbf{A}_2$.
- S.t., $\mathsf{HEval}[f](\mathbf{A}, \mathbf{M}, x) = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) - f(x) \otimes \mathbf{G}$.

Attribute-based LFE (AB-LFE)

Syntax: (ABE-like, public x and secret μ)



Properties:

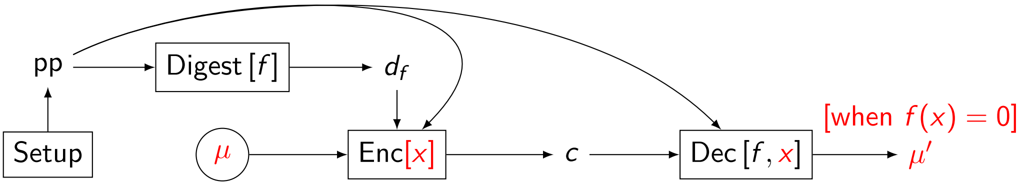
- Correctness: $\mu' = \mu$ when $f(x) = 0$.
- Security: c hides μ.

Interpretation: LFE for "conditional disclosure" $\hat{f}(x, \mu) := (x, \mu \cdot (1 - f(x)))$.

Generalization: $f(x) \in \{0, 1\}^O$, have $\mu_1, \ldots, \mu_O$, and require $\mu'_j = \mu_j$ when $f_j(x) = 0$.

Attribute-based LFE (AB-LFE)

Syntax: (ABE-like, public x and secret μ)



Properties:

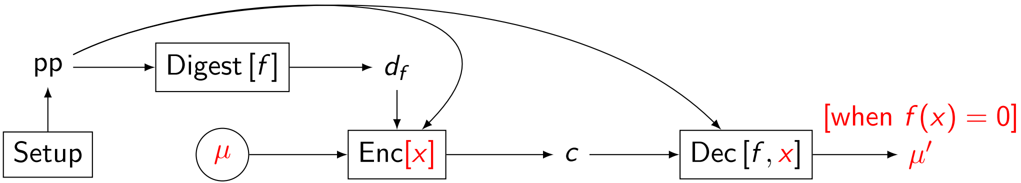
- Correctness: $\mu' = \mu$ when $f(x) = 0$.
- Security: c hides μ.

Interpretation: LFE for "conditional disclosure" $\hat{f}(x, \mu) := (x, \mu \cdot (1 - f(x)))$.

Generalization: $f(x) \in \{0,1\}^O$, have $\mu_1, \ldots, \mu_O$, and require $\mu'_j = \mu_j$ when $f_j(x) = 0$.

Attribute-based LFE (AB-LFE)

Syntax: (ABE-like, public x and secret μ)



Properties:

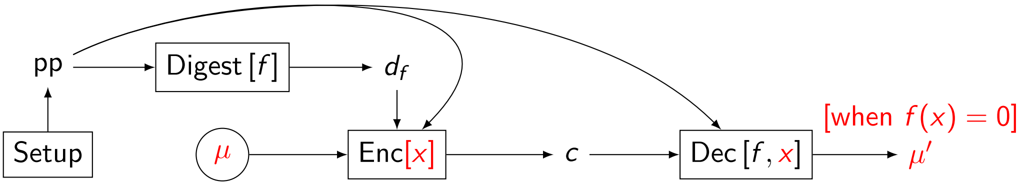
- Correctness: $\mu' = \mu$ when $f(x) = 0$.
- Security: c hides μ.

Interpretation: LFE for "conditional disclosure" $\hat{f}(x, \mu) := (x, \mu \cdot (1 - f(x)))$.

Generalization: $f(x) \in \{0,1\}^O$, have $\mu_1, \ldots, \mu_O$, and require $\mu'_j = \mu_j$ when $f_j(x) = 0$.

Attribute-based LFE (AB-LFE)

Syntax: (ABE-like, public x and secret μ)



Properties:

- Correctness: $\mu' = \mu$ when $f(x) = 0$.
- Security: c hides μ.

Interpretation: LFE for "conditional disclosure" $\hat{f}(x, \mu) := (x, \mu \cdot (1 - f(x)))$.

Generalization: $f(x) \in \{0,1\}^O$, have $\mu_1, \ldots, \mu_O$, and require $\mu'_j = \mu_j$ when $f_j(x) = 0$.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top (\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest$(\mathbf{M}, f)$: $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc$(\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L})$: sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec$(\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu))$: compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): $\mathsf{pp} = \mathbf{M} \leftarrow \mathbb{Z}_q^{n \times In\ell}$.
- Digest($\mathbf{M}, f$): $d_f = \mathbf{M}_f = \mathsf{HEval}^{\mathsf{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n \times On\ell}$.
- Enc($\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O \cdot L}$): sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n \times L})) \in \{0,1\}^{n\ell \times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathsf{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec($\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$): compute $\mathbf{c}_{f,x}^\top = \mathsf{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

AB-LFE from LWE

Construction: Suppose $f : \{0,1\}^I \to \{0,1\}^O$.

- Setup(1^n): pp $= \mathbf{M} \leftarrow \mathbb{Z}_q^{n\times In\ell}$.
- Digest$(\mathbf{M}, f)$: $d_f = \mathbf{M}_f = \mathrm{HEval}^{\mathrm{pub}}[f](\mathbf{M}) \in \mathbb{Z}_q^{n\times On\ell}$.
- Enc$(\mathbf{M}, \mathbf{M}_f, x, \mu \in \{0,1\}^{O\cdot L})$: sample $\mathbf{s} \leftarrow \mathbb{Z}_q^n$ and LWE errors $\mathbf{e}_x, \mathbf{e}_\mu$, sample $\mathbf{R}_j \leftarrow \mathbf{G}^{-1}(U(\mathbb{Z}_q^{n\times L})) \in \{0,1\}^{n\ell\times L}$, output $c = (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu)$ where $\mathbf{R} = \mathrm{diag}(\{\mathbf{R}_j\}_j)$,

$$\mathbf{c}_x^\top = \mathbf{s}^\top \underbrace{(\mathbf{M} - x \otimes \mathbf{G})}_{\mathbf{A}} + \mathbf{e}_x^\top \in \mathbb{Z}_q^{In\ell}, \qquad \mathbf{c}_\mu^\top = \mathbf{s}^\top \mathbf{M}_f \mathbf{R} + \mathbf{e}_\mu^\top + \lfloor q/2 \rceil \cdot \mu \in \mathbb{Z}_q^{OL}.$$

- Dec$(\mathbf{M}, f, x, (\mathbf{R}, \mathbf{c}_x, \mathbf{c}_\mu))$: compute $\mathbf{c}_{f,x}^\top = \mathrm{HEval}[f](\mathbf{c}_x^\top, \mathbf{M}, x)$, and for $f_j(x) = 0$, extract μ_j by checking $|\mathbf{c}_{f,x}^\top \mathbf{R} - \mathbf{c}_\mu^\top| > q/4$ on the j-th block.

Correctness: by $\mathbf{c}_{f,x}^\top \approx \mathbf{s}^\top(\mathbf{M}_f - f(x) \otimes \mathbf{G})$. Security: by LWE.

Enhancing AB-LFE

Two-outcome mode of ABE/AB-LFE:

- Normal mode: Dec outputs μ if $f(x) = 0$ and $\perp$ otherwise.
- Two-outcome mode: Enc takes $\mu^{(0)}, \mu^{(1)}$, and Dec outputs $\mu^{(f(x))}$.
- Construction: apply ABX to $\tilde{f} := f \parallel (1 - f)$.

Further compressing digest: By *laconic OT* [CDG+17], can improve $|d_f|$ from $O \cdot \mathrm{poly}(n, d)$ (d is depth of f) to just $\mathrm{poly}(n)$.

Enhancing AB-LFE

Two-outcome mode of ABE/AB-LFE:

- Normal mode: Dec outputs μ if $f(x) = 0$ and $\perp$ otherwise.
- Two-outcome mode: Enc takes $\mu^{(0)}, \mu^{(1)}$, and Dec outputs $\mu^{(f(x))}$.
- Construction: apply ABX to $\tilde{f} := f \parallel (1 - f)$.

Further compressing digest: By *laconic OT* [CDG+17], can improve $|d_f|$ from $O \cdot \text{poly}(n, d)$ (d is depth of f) to just $\text{poly}(n)$.

Enhancing AB-LFE

Two-outcome mode of ABE/AB-LFE:

- Normal mode: Dec outputs μ if $f(x) = 0$ and $\perp$ otherwise.
- Two-outcome mode: Enc takes $\mu^{(0)}, \mu^{(1)}$, and Dec outputs $\mu^{(f(x))}$.
- Construction: apply ABX to $\tilde{f} := f \parallel (1 - f)$.

Further compressing digest: By *laconic OT* [CDG+17], can improve $|d_f|$ from $O \cdot \text{poly}(n, d)$ (d is depth of f) to just $\text{poly}(n)$.

Last Piece: Garbled Circuit

Syntax: $(f : \{0,1\}^I \to \{0,1\}^O.)$

- Garble$(1^n, f)$: output garbled circuit Γ and labels $(L_{i,0}, L_{i,1})_{i\in[I]}$.
- GEval$(\Gamma, (L_i)_{i\in[I]})$: output evaluation y.

Correctness: GEval$(\Gamma, (L_{i,x_i})_{i\in[I]}) = f(x)$.

Yao's construction: gate by gate, so $|\Gamma| = |f| \cdot \text{poly}(n)$; also $|L_{i,b}| = \text{poly}(n)$.

Last Piece: Garbled Circuit

Syntax: $(f : \{0,1\}^I \to \{0,1\}^O.)$

- Garble$(1^n, f)$: output garbled circuit Γ and labels $(L_{i,0}, L_{i,1})_{i \in [I]}$.
- GEval$(\Gamma, (L_i)_{i \in [I]})$: output evaluation y.

Correctness: GEval$(\Gamma, (L_{i,x_i})_{i \in [I]}) = f(x)$.

Yao's construction: gate by gate, so $|\Gamma| = |f| \cdot \mathrm{poly}(n)$; also $|L_{i,b}| = \mathrm{poly}(n)$.

Last Piece: Garbled Circuit

Syntax: $(f : \{0,1\}^I \to \{0,1\}^O.)$

- Garble$(1^n, f)$: output garbled circuit Γ and labels $(L_{i,0}, L_{i,1})_{i\in[I]}$.
- GEval$(\Gamma, (L_i)_{i\in[I]})$: output evaluation y.

Correctness: GEval$(\Gamma, (L_{i,x_i})_{i\in[I]}) = f(x)$.

Yao's construction: gate by gate, so $|\Gamma| = |f| \cdot \text{poly}(n)$; also $|L_{i,b}| = \text{poly}(n)$.

Last Piece: Garbled Circuit

Syntax: $(f : \{0,1\}^I \to \{0,1\}^O.)$

- $\mathsf{Garble}(1^n, f)$: output garbled circuit Γ and labels $(L_{i,0}, L_{i,1})_{i \in [I]}$.
- $\mathsf{GEval}(\Gamma, (L_i)_{i \in [I]})$: output evaluation y.

Correctness: $\mathsf{GEval}(\Gamma, (L_{i,x_i})_{i \in [I]}) = f(x)$.

Yao's construction: gate by gate, so $|\Gamma| = |f| \cdot \mathrm{poly}(n)$; also $|L_{i,b}| = \mathrm{poly}(n)$.

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- Setup(1^n): same as toABLFE.Setup.
- Digest(pp, f): $f^\dagger :=$ FHE.HEval[f], output $d_f =$ toABLFE.Digest(pp, $f^\dagger$).
- Enc(pp, d_f, x):
  sample FHE secret $k \leftarrow$ FHE.Gen(1^n), compute $c_x =$ FHE.Enc(k, x),
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) =$ Garble(1^n, FHE.Dec($k, \cdot$)),
  compute $c =$ toABLFE.Enc(pp, $d_f, c_x, (L_{i,0})_i, (L_{i,1})_i$),
  output $c' = (\Gamma, c)$.
- Dec(pp, f, (Γ, c)): $(L_i)_i =$ toABLFE.Dec(pp, $f^\dagger$, c), output $y =$ GEval($\Gamma, (L_i)_i$).

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- Setup(1^n): same as toABLFE.Setup.
- Digest(pp, f): $f^\dagger :=$ FHE.HEval[f], output $d_f =$ toABLFE.Digest(pp, $f^\dagger$).
- Enc(pp, d_f, x):
  sample FHE secret $k \leftarrow$ FHE.Gen(1^n), compute $c_x =$ FHE.Enc(k, x),
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) =$ Garble(1^n, FHE.Dec($k, \cdot$)),
  compute $c =$ toABLFE.Enc(pp, $d_f, c_x, (L_{i,0})_i, (L_{i,1})_i$),
  output $c' = (\Gamma, c)$.
- Dec(pp, $f, (\Gamma, c)$): $(L_i)_i =$ toABLFE.Dec(pp, $f^\dagger, c$), output $y =$ GEval($\Gamma, (L_i)_i$).

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- Setup(1^n): same as toABLFE.Setup.
- Digest(pp, f): $f^\dagger :=$ FHE.HEval[f], output $d_f =$ toABLFE.Digest(pp, $f^\dagger$).
- Enc(pp, d_f, x):
  sample FHE secret $k \leftarrow$ FHE.Gen(1^n), compute $c_x =$ FHE.Enc(k, x),
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) =$ Garble(1^n, FHE.Dec($k, \cdot$)),
  compute $c =$ toABLFE.Enc(pp, $d_f, c_x, (L_{i,0})_i, (L_{i,1})_i$),
  output $c' = (\Gamma, c)$.
- Dec(pp, f, (Γ, c)): $(L_i)_i =$ toABLFE.Dec(pp, $f^\dagger$, c), output $y =$ GEval($\Gamma, (L_i)_i$).

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- Setup(1^n): same as toABLFE.Setup.
- Digest(pp, f): $f^\dagger :=$ FHE.HEval[f], output $d_f =$ toABLFE.Digest(pp, $f^\dagger$).
- Enc(pp, d_f, x):
  sample FHE secret $k \leftarrow$ FHE.Gen(1^n), compute $c_x =$ FHE.Enc(k, x),
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) =$ Garble(1^n, FHE.Dec($k, \cdot$)),
  compute $c =$ toABLFE.Enc(pp, $d_f, c_x, (L_{i,0})_i, (L_{i,1})_i$),
  output $c' = (\Gamma, c)$.
- Dec(pp, f, (Γ, c)): $(L_i)_i =$ toABLFE.Dec(pp, $f^\dagger$, c), output $y =$ GEval($\Gamma, (L_i)_i$).

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- Setup(1^n): same as toABLFE.Setup.
- Digest(pp, f): $f^\dagger :=$ FHE.HEval[f], output $d_f =$ toABLFE.Digest(pp, $f^\dagger$).
- Enc(pp, d_f, x):
  sample FHE secret $k \leftarrow$ FHE.Gen(1^n), compute $c_x =$ FHE.Enc(k, x),
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) =$ Garble(1^n, FHE.Dec($k, \cdot$)),
  compute $c =$ toABLFE.Enc(pp, $d_f, c_x, (L_{i,0})_i, (L_{i,1})_i$),
  output $c' = (\Gamma, c)$.
- Dec(pp, f, (Γ, c)): $(L_i)_i =$ toABLFE.Dec(pp, $f^\dagger$, c), output $y =$ GEval($\Gamma, (L_i)_i$).

Constructing LFE

Ingredients: two-outcome AB-LFE (toABLFE), FHE, garbled circuit (GC).

Construction:

- $\mathsf{Setup}(1^n)$: same as toABLFE.Setup.
- $\mathsf{Digest}(\mathsf{pp}, f)$: $f^\dagger := \mathsf{FHE.HEval}[f]$, output $d_f = \mathsf{toABLFE.Digest}(\mathsf{pp}, f^\dagger)$.
- $\mathsf{Enc}(\mathsf{pp}, d_f, x)$:
  sample FHE secret $k \leftarrow \mathsf{FHE.Gen}(1^n)$, compute $c_x = \mathsf{FHE.Enc}(k, x)$,
  compute $(\Gamma, (L_{i,0}, L_{i,1})_i) = \mathsf{Garble}(1^n, \mathsf{FHE.Dec}(k, \cdot))$,
  compute $c = \mathsf{toABLFE.Enc}(\mathsf{pp}, d_f, c_x, (L_{i,0})_i, (L_{i,1})_i)$,
  output $c' = (\Gamma, c)$.
- $\mathsf{Dec}(\mathsf{pp}, f, (\Gamma, c))$: $(L_i)_i = \mathsf{toABLFE.Dec}(\mathsf{pp}, f^\dagger, c)$, output $y = \mathsf{GEval}(\Gamma, (L_i)_i)$.

Verifying the Correctness

$$f^\dagger := \mathsf{FHE.HEval}[f]\ , \qquad d_f = \mathsf{toABLFE.Digest}(\mathsf{pp}, f^\dagger)\ ,$$
$$c_x = \mathsf{FHE.Enc}(k, x)\ , \qquad (\Gamma, (L_{i,0}, L_{i,1})_i) = \mathsf{Garble}(1^n, \mathsf{FHE.Dec}(k, \cdot))\ ,$$
$$c = \mathsf{toABLFE.Enc}(\mathsf{pp}, d_f, c_x, (L_{i,0})_i, (L_{i,1})_i)\ ,$$
$$(L_i)_i = \mathsf{toABLFE.Dec}(\mathsf{pp}, f^\dagger, c)\ , \qquad y = \mathsf{GEval}(\Gamma, (L_i)_i)\ .$$

Want: $y = f(x)$.

- By toABLFE, $L_i = L_{i, f^\dagger(c_x)[i]}$.
- By FHE, $f^\dagger(c_x) = \mathsf{FHE.HEval}[f](c_x) = c_{f(x)}$.
- By GC, $\mathsf{GEval}(\Gamma, (L_{i, c_{f(x)}[i]})_i) = \mathsf{FHE.Dec}(k, c_{f(x)}) = f(x)$.

Verifying the Correctness

$$
\begin{gathered}
f^\dagger := \mathsf{FHE.HEval}[f] \ , \qquad d_f = \mathsf{toABLFE.Digest}(\mathsf{pp}, f^\dagger) \ , \\
c_x = \mathsf{FHE.Enc}(k, x) \ , \qquad (\Gamma, (L_{i,0}, L_{i,1})_i) = \mathsf{Garble}(1^n, \mathsf{FHE.Dec}(k, \cdot)) \ , \\
c = \mathsf{toABLFE.Enc}(\mathsf{pp}, d_f, c_x, (L_{i,0})_i, (L_{i,1})_i) \ , \\
(L_i)_i = \mathsf{toABLFE.Dec}(\mathsf{pp}, f^\dagger, c) \ , \qquad y = \mathsf{GEval}(\Gamma, (L_i)_i) \ .
\end{gathered}
$$

Want: $y = f(x)$.

- By toABLFE, $L_i = L_{i, f^\dagger(c_x)[i]}$.
- By FHE, $f^\dagger(c_x) = \mathsf{FHE.HEval}[f](c_x) = c_{f(x)}$.
- By GC, $\mathsf{GEval}(\Gamma, (L_{i, c_{f(x)}[i]})_i) = \mathsf{FHE.Dec}(k, c_{f(x)}) = f(x)$.

Verifying the Correctness

$$f^\dagger := \mathsf{FHE.HEval}[f] \;, \qquad d_f = \mathsf{toABLFE.Digest}(\mathsf{pp}, f^\dagger) \;,$$
$$c_x = \mathsf{FHE.Enc}(k, x) \;, \qquad (\Gamma, (L_{i,0}, L_{i,1})_i) = \mathsf{Garble}(1^n, \mathsf{FHE.Dec}(k, \cdot)) \;,$$
$$c = \mathsf{toABLFE.Enc}(\mathsf{pp}, d_f, c_x, (L_{i,0})_i, (L_{i,1})_i) \;,$$
$$(L_i)_i = \mathsf{toABLFE.Dec}(\mathsf{pp}, f^\dagger, c) \;, \qquad y = \mathsf{GEval}(\Gamma, (L_i)_i) \;.$$

Want: $y = f(x)$.

- By toABLFE, $L_i = L_{i, f^\dagger(c_x)[i]}$.
- By FHE, $f^\dagger(c_x) = \mathsf{FHE.HEval}[f](c_x) = c_{f(x)}$.
- By GC, $\mathsf{GEval}(\Gamma, (L_{i, c_{f(x)}[i]})_i) = \mathsf{FHE.Dec}(k, c_{f(x)}) = f(x)$.

Verifying the Correctness

$$f^\dagger := \mathsf{FHE.HEval}[f] \;, \qquad d_f = \mathsf{toABLFE.Digest}(\mathsf{pp}, f^\dagger) \;,$$
$$c_x = \mathsf{FHE.Enc}(k, x) \;, \qquad (\Gamma, (L_{i,0}, L_{i,1})_i) = \mathsf{Garble}(1^n, \mathsf{FHE.Dec}(k, \cdot)) \;,$$
$$c = \mathsf{toABLFE.Enc}(\mathsf{pp}, d_f, c_x, (L_{i,0})_i, (L_{i,1})_i) \;,$$
$$(L_i)_i = \mathsf{toABLFE.Dec}(\mathsf{pp}, f^\dagger, c) \;, \qquad y = \mathsf{GEval}(\Gamma, (L_i)_i) \;.$$

Want: $y = f(x)$.

- By toABLFE, $L_i = L_{i, f^\dagger(c_x)[i]}$.
- By FHE, $f^\dagger(c_x) = \mathsf{FHE.HEval}[f](c_x) = c_{f(x)}$.
- By GC, $\mathsf{GEval}(\Gamma, (L_{i, c_{f(x)}[i]})_i) = \mathsf{FHE.Dec}(k, c_{f(x)}) = f(x)$.

Verifying the Efficiency

Unpack the construction:

- $f^\dagger :=$ FHE.HEval$[f]$, toABLFE uses $\widetilde{f^\dagger} :=$ FHE.HEval$[f] \parallel (1 -$ FHE.HEval$[f])$.

  (Need to binary-compile FHE.HEval.)

- For $f : \{0,1\}^I \to \{0,1\}^O$, get $\widetilde{f^\dagger} : \{0,1\}^{I \cdot \mathrm{poly}(n,d)} \to \{0,1\}^{2O \cdot \mathrm{poly}(n,d)}$.

Hence $|\mathrm{pp}| = I \cdot \mathrm{poly}(n,d)$, and $|d_f| = O \cdot \mathrm{poly}(n,d)$ (or $|d_f| = \mathrm{poly}(n)$ with LOT).

Verifying the Efficiency

Unpack the construction:

- $f^\dagger :=$ FHE.HEval$[f]$, toABLFE uses $\widetilde{f^\dagger} :=$ FHE.HEval$[f] \parallel (1 -$ FHE.HEval$[f])$.
  (Need to binary-compile FHE.HEval.)
- For $f : \{0,1\}^I \to \{0,1\}^O$, get $\widetilde{f^\dagger} : \{0,1\}^{I \cdot \mathrm{poly}(n,d)} \to \{0,1\}^{2O \cdot \mathrm{poly}(n,d)}$.

Hence $|\mathrm{pp}| = I \cdot \mathrm{poly}(n,d)$, and $|d_f| = O \cdot \mathrm{poly}(n,d)$ (or $|d_f| = \mathrm{poly}(n)$ with LOT).

Verifying the Efficiency

Unpack the construction:

- $f^\dagger :=$ FHE.HEval[f], toABLFE uses $\widetilde{f^\dagger} :=$ FHE.HEval[f] $\|$ (1 − FHE.HEval[f]).
  (Need to binary-compile FHE.HEval.)
- For $f : \{0,1\}^I \to \{0,1\}^O$, get $\widetilde{f^\dagger} : \{0,1\}^{I \cdot \mathrm{poly}(n,d)} \to \{0,1\}^{2O \cdot \mathrm{poly}(n,d)}$.

Hence $|\mathrm{pp}| = I \cdot \mathrm{poly}(n,d)$, and $|d_f| = O \cdot \mathrm{poly}(n,d)$ (or $|d_f| = \mathrm{poly}(n)$ with LOT).

Verifying the Efficiency

Unpack the construction:

- $f^\dagger :=$ FHE.HEval$[f]$, toABLFE uses $\widetilde{f^\dagger} :=$ FHE.HEval$[f] \parallel (1 -$ FHE.HEval$[f])$.
  (Need to binary-compile FHE.HEval.)
- For $f : \{0,1\}^I \to \{0,1\}^O$, get $\widetilde{f^\dagger} : \{0,1\}^{I \cdot \mathrm{poly}(n,d)} \to \{0,1\}^{2O \cdot \mathrm{poly}(n,d)}$.

Hence $|\mathrm{pp}| = I \cdot \mathrm{poly}(n,d)$, and $|d_f| = O \cdot \mathrm{poly}(n,d)$ (or $|d_f| = \mathrm{poly}(n)$ with LOT).

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0,1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0, 1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0,1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0, 1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0, 1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i \in [N]} r_{i,j} \mathbf{H}_i)_{j \in [O]}$ for $r_{i,j} \leftarrow \{0,1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top \mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top (\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top (\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top (c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

Enhancing LFE

Adaptive security: by assuming certain adaptive version of LWE.

(Statistical) function hiding:

- Add $\mathbf{H} \in \mathbb{Z}_q^{n \times Nn\ell}$ to pp, use $d'_f = d_f + (\sum_{i\in[N]} r_{i,j}\mathbf{H}_i)_{j\in[O]}$ for $r_{i,j} \leftarrow \{0,1\}$.
- Also encrypt $\mathbf{c}_H^\top = \mathbf{s}^\top\mathbf{H} + \mathbf{e}_H^\top = \mathbf{s}^\top(\mathbf{H} - 0 \otimes \mathbf{G}) + \mathbf{e}_H^\top$.
- Interpretation: hide f by $f'(x, x') := f(x) + x' \cdot \mathbf{R}$ (over $\mathbb{Z}_q$ integers), $\mathbf{R} = (r_{i,j})_{i,j}$.

More direct construction:

- "Dual use" technique [BTVW17]: take GSW FHE, reuse key $\mathbf{s}$ in ABLFE.Enc.
- No garbling, directly encrypt $\mathbf{s}^\top(\mathbf{M} - c_x \otimes \mathbf{G}) + \mathbf{e}_x^\top$.
- "Automatic decryption": by GSW, can extract $f(x)$ from $\mathbf{s}^\top(c_{f(x)} \otimes \mathbf{G}) + \mathbf{e}^\top$.

References

Dan Boneh, Craig Gentry, Sergey Gorbunov, Shai Halevi, Valeria Nikolaenko, Gil Segev, Vinod Vaikuntanathan, and Dhinakaran Vinayagamurthy.
Fully key-homomorphic encryption, arithmetic circuit ABE, and compact garbled circuits.
In *EUROCRYPT*, 2014.

Zvika Brakerski, Rotem Tsabary, Vinod Vaikuntanathan, and Hoeteck Wee.
Private constrained PRFs (and more) from LWE.
In *TCC*, 2017.

Chongwon Cho, Nico Döttling, Sanjam Garg, Divya Gupta, Peihan Miao, and Antigoni Polychroniadou.
Laconic oblivious transfer and its applications.
In *CRYPTO*, 2017.

Shafi Goldwasser, Yael Kalai, Raluca Ada Popa, Vinod Vaikuntanathan, and Nickolai Zeldovich.
Reusable garbled circuits and succinct functional encryption.
In *STOC*, 2013.

Craig Gentry, Amit Sahai, and Brent Waters.
Homomorphic encryption from learning with errors: Conceptually-simpler, asymptotically-faster, attribute-based.
In *CRYPTO*, 2013.

Willy Quach, Hoeteck Wee, and Daniel Wichs.
Laconic function evaluation and applications.
In *FOCS*, 2018.