Functional Commitments and SNARGs for P/poly from SIS

Hoeteck Wee
NTT Research

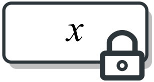
functional commitment **(FC)**

[LRY16, IKO07]

functional commitment **(FC)**

[LRY16, IKO07]

$$\textbf{commit}(\textbf{crs}, x) \mapsto \sigma$$



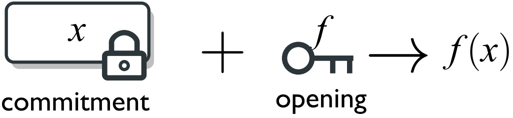
commitment

functional commitment **(FC)**

[LRY16, IKO07]

$$\textbf{commit}(\textbf{crs}, x) \mapsto \sigma$$

$$\textbf{open}(x, f) \mapsto \pi$$



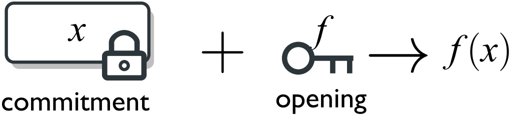
functional commitment **(FC)**

[LRY16, IKO07]

$\textbf{commit}(\textbf{crs}, x) \mapsto \sigma$

$\textbf{open}(x, f) \mapsto \pi$

$\textbf{verify}(\textbf{crs}, \sigma, f, \pi, y) \mapsto 0/1 \quad y \stackrel{?}{=} f(x)$



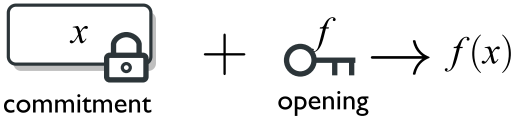
functional commitment **(FC)**

[LRY16, IKO07]

commit(**crs**, x) $\mapsto \sigma$ **small** $\ll |x|$

open(x, f) $\mapsto \pi$ **small** $\ll |x|$

verify(**crs**, σ, f, π, y) $\mapsto 0/1$ **fast** $\ll$ time(f)



functional commitment **(FC)**

[LRY16, IKO07]

$\textbf{commit}(\textbf{crs}, x) \mapsto \sigma$ **small** $\ll |x|$

$\textbf{open}(x, f) \mapsto \pi$ **small** $\ll |x|$

$\textbf{verify}(\textbf{crs}, \sigma, f, \pi, y) \mapsto 0/1$ **fast** $\ll \text{time}(f)$

---

binding. hard to find σ that open to $y_0 \neq y_1$

this work

functional commitments for P/poly from SIS

$|\textbf{crs}| = O(1)$

$|\textbf{commitment}| = O(1)$

$|\textbf{opening}| = O(\text{depth})$

this work

functional commitments for P/poly from SIS

$|\textbf{crs}| = O(1)$ **transparent**

$|\textbf{commitment}| = O(1)$

$|\textbf{opening}| = O(\text{depth})$

verification time $O(|x|)$ (after pre-processing)

this work

functional commitments for P/poly from SIS

$|\textbf{crs}| = O(1)$ **transparent**

$|\textbf{commitment}| = O(1)$

$|\textbf{opening}| = O(\text{depth})$

verification time $O(|x|)$ (after pre-processing)

prior. non-standard SIS, poly(depth) factors

[ACLMT22, WW23, BCFL23, CLM23, FLV23, W25]

this work (**II**)

SNARGs for P/poly from SIS

... **NO** random oracles

this work (**II**)

SNARGs for P/poly from SIS

$|\textbf{crs}| = O(1)$

$|\textbf{proof}| = O(\text{depth})$

verification time $O(|x|)$ (after pre-processing)

this work (II)

SNARGs for P/poly from SIS

$|\textbf{crs}| = O(1)$ **transparent**

$|\textbf{proof}| = O(\text{depth})$ **unambiguous** **[KPY20]**

verification time $O(|x|)$ (after pre-processing)

this work (II)

SNARGs for P/poly from SIS

$|\textbf{crs}| = O(1)$ **transparent**

$|\textbf{proof}| = O(\text{depth})$ **unambiguous** **[KPY20]**

verification time $O(|x|)$ (after pre-processing)

✓ first SNARG from Minicrypt assumption

✓ **NO** Fiat-Shamir, CI-hashing, PCPs, BARGs

[JKKZ21, CJJ21, KLVW23, KLV23, CGJJZ23]

SIS assumption [A96]

SIS. given $\mathbf{B} \leftarrow \mathbb{Z}_q^{n \times m}$, hard to find a low-norm $\mathbf{z} \neq \mathbf{0}$ s.t. $\mathbf{B}\mathbf{z} = \mathbf{0} \bmod q$.

warm-up [WW23,W24]

functional commitments from succinct SIS

$|\textbf{crs}| = O_{\text{depth}}(\ell^2)$ where $\ell = |x|$

$|\textbf{commitment}| = O_{\text{depth}}(1)$

$|\textbf{opening}| = O_{\text{depth}}(1)$

slow verification

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, i,j \in [\ell]$

$\mathbf{B}$ $\quad$ $\mathbf{W}_j \in \mathbb{Z}_q^{n \times m}$

$\mathbf{V}_i \in \{0,1\}^{m \times m}$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, i,j \in [\ell]$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, i,j \in [\ell]$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

open(x, f):

1. compute low-norm $\mathbf{Z}_i$ s.t.

$\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$ **GSW.enc**$(\mathbf{B}, x_i)$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

open(x, f):

1. compute low-norm $\mathbf{Z}_i$ s.t.

$\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$ **GSW.enc**$(\mathbf{B}, x_i)$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

open(x, f):

1. compute low-norm $\mathbf{Z}_i$ s.t.

$\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$ **GSW.enc**$(\mathbf{B}, x_i)$

2. homomorphic eval [GSW13,BGGHNSVV14,GVW15]

$\rightarrow \mathbf{C}_f = \mathbf{B}\mathbf{Z}_f + f(x)\mathbf{G}$ **GSW.enc**$(\mathbf{B}, f(x))$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

open(x, f): $\mathbf{Z}_f$

1. compute low-norm $\mathbf{Z}_i$ s.t.

$\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$ **GSW.enc**$(\mathbf{B}, x_i)$

2. homomorphic eval [GSW13,BGGHNSVV14,GVW15]

$\rightarrow \mathbf{C}_f = \mathbf{B}\mathbf{Z}_f + f(x)\mathbf{G}$ **GSW.enc**$(\mathbf{B}, f(x))$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

open(x, f): $\mathbf{Z}_f$

verify: $\mathbf{C}_f \stackrel{?}{=} \mathbf{B}\mathbf{Z} + y\mathbf{G}$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

next. relax $\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$ cf.[AMR25a]

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

next. relax $\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$

✓ binding from standard SIS

+ transparent set-up

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

next. relax $\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$

- ✓ binding from standard SIS
- ✗ $\mathbf{C}\mathbf{V}_i \neq$ **GSW.enc**$(\mathbf{B}, x_i)$
- ✗ $\mathbf{Z}_i$ have size $O(\ell^2)$, not $O(1)$

warm-up [WW23,W24]

crs: $\mathbf{B}, \mathbf{W}_j, \mathbf{V}_i, \mathbf{B}^{-1}(\mathbf{W}_j\mathbf{V}_i - \delta_{ij}\mathbf{G})$

commit(x): $\mathbf{C} = \sum x_j \mathbf{W}_j$

next. relax $\mathbf{C}\mathbf{V}_i = \mathbf{B}\mathbf{Z}_i + x_i\mathbf{G}$

✓ binding from standard SIS ①

✗ $\mathbf{C}\mathbf{V}_i \neq$ **GSW.enc**$(\mathbf{B}, x_i)$ ②

✗ $\mathbf{Z}_i$ have size $O(\ell^2)$, not $O(1)$ ③

❶ commitment from **SIS**

relax. $\mathbf{CV}_i = \mathbf{BZ}_i + x_i\mathbf{G}$

➊ commitment from **SIS**

relax. $\mathbf{C}\mathbf{V}_i - x_i\mathbf{G} = \mathbf{B}\mathbf{Z}_i$

❶ commitment from **SIS**

relax. $\mathbf{CV}_i - x_i\mathbf{G} = \mathbf{BZ}_i$

i. $\mathbf{CV}_i - x_i\mathbf{G} \mapsto \begin{bmatrix} \mathbf{CV}_i \\ -x_i\mathbf{G} \end{bmatrix}$

❶ commitment from **SIS**

relax. $\mathbf{C}\mathbf{V}_i - x_i\mathbf{G} = \mathbf{B}\mathbf{Z}_i$

i. $\mathbf{C}\mathbf{V}_i - x_i\mathbf{G} \mapsto \begin{bmatrix} \mathbf{C}\mathbf{V}_i \\ -x_i\mathbf{G} \end{bmatrix}$

ii. $\mathbf{B} = \begin{bmatrix} \cdots & \mathbf{W}_i\mathbf{V}_j & \cdots \\ \cdots & -\delta_{ij}\mathbf{G} & \cdots \end{bmatrix} \in \mathbb{Z}_q^{2n \times \ell^2 m}$

❶ commitment from **SIS**

crs: $\mathbf{W}_j, \mathbf{V}_i$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_i \\ -x_i\mathbf{G} \end{bmatrix} = \overbrace{\begin{bmatrix} \cdots & \mathbf{W}_i\mathbf{V}_j & \cdots \\ \cdots & -\delta_{ij}\mathbf{G} & \cdots \end{bmatrix}}^{\mathbf{B}} \mathbf{Z}_i$$

❶ commitment from **SIS**

crs: $\mathbf{W}_j, \mathbf{V}_i$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_i \\ -x_i\mathbf{G} \end{bmatrix} = \overbrace{\begin{bmatrix} \cdots & \mathbf{W}_i\mathbf{V}_j & \cdots \\ \cdots & -\delta_{ij}\mathbf{G} & \cdots \end{bmatrix}}^{\mathbf{B}} \mathbf{Z}_i$$

correctness.

$$\begin{bmatrix} (\sum x_j \mathbf{W}_j)\mathbf{V}_i \\ -x_i\mathbf{G} \end{bmatrix} = \begin{bmatrix} \mathbf{W}_i\mathbf{V}_i \\ -\mathbf{G} \end{bmatrix} x_i + \sum_{j \neq i} \begin{bmatrix} \mathbf{W}_j\mathbf{V}_i \\ \mathbf{0} \end{bmatrix} x_j$$

❶ commitment from **SIS**

crs: $\mathbf{W}_j, \mathbf{V}_i$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_i \\ -x_i\mathbf{G} \end{bmatrix} = \overbrace{\begin{bmatrix} \cdots & \mathbf{W}_i\mathbf{V}_j & \cdots \\ \cdots & -\delta_{ij}\mathbf{G} & \cdots \end{bmatrix}}^{\mathbf{B}} \mathbf{Z}_i$$

binding.

SIS $\Rightarrow \overline{\mathbf{B}} = \begin{bmatrix} \cdots & \mathbf{W}_i\mathbf{V}_j & \cdots \end{bmatrix}$ is SIS-hard

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{CV}_1 \\ -x_1\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_1$$

$$\begin{bmatrix} \mathbf{CV}_2 \\ -x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_2$$

goal. $$\begin{bmatrix} \mathbf{CV}_{12} \\ -x_1 x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_{12}$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{CV}_1 \\ -x_1\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_1$$

$$\begin{bmatrix} x_1\mathbf{CV}_2 \\ -x_1x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot x_1\mathbf{Z}_2$$

goal. $$\begin{bmatrix} \mathbf{CV}_{12} \\ -x_1x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_{12}$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ -x_1\mathbf{C}\mathbf{V}_2 \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2)$$

$$\begin{bmatrix} x_1\mathbf{C}\mathbf{V}_2 \\ -x_1x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot x_1\mathbf{Z}_2$$

goal. $$\begin{bmatrix} \mathbf{C}\mathbf{V}_{12} \\ -x_1x_2\mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_{12}$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_1 \mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ -x_1 \mathbf{C}\mathbf{V}_2 \end{bmatrix} = \begin{bmatrix} \overline{\mathbf{B}} \\ \underline{\mathbf{B}} \end{bmatrix} \cdot \mathbf{Z}_1 \mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2)$$

$$\begin{bmatrix} x_1 \mathbf{C}\mathbf{V}_2 \\ -x_1 x_2 \mathbf{G} \end{bmatrix} = \begin{bmatrix} \overline{\mathbf{B}} \\ \underline{\mathbf{B}} \end{bmatrix} \cdot x_1 \mathbf{Z}_2$$

goal. $$\begin{bmatrix} \mathbf{C}\mathbf{V}_{12} \\ -x_1 x_2 \mathbf{G} \end{bmatrix} = \mathbf{B} \cdot \mathbf{Z}_{12}$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ -x_1\mathbf{C}\mathbf{V}_2 \\ \mathbf{0} \end{bmatrix} = \begin{bmatrix} \overline{\mathbf{B}} \\ \underline{\mathbf{B}} \\ \mathbf{0} \end{bmatrix} \cdot \mathbf{Z}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2)$$

$$\begin{bmatrix} \mathbf{0} \\ x_1\mathbf{C}\mathbf{V}_2 \\ -x_1x_2\mathbf{G} \end{bmatrix} = \begin{bmatrix} \mathbf{0} \\ \overline{\mathbf{B}} \\ \underline{\mathbf{B}} \end{bmatrix} \cdot x_1\mathbf{Z}_2$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ \mathbf{0} \\ -x_1x_2\mathbf{G} \end{bmatrix} = \begin{bmatrix} \overline{\mathbf{B}} & \\ \underline{\mathbf{B}} & \overline{\mathbf{B}} \\ & \underline{\mathbf{B}} \end{bmatrix} \overbrace{\begin{bmatrix} \mathbf{Z}_1\mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ x_1\mathbf{Z}_2 \end{bmatrix}}^{\mathbf{Z}_{12}}$$

② multiplication $x_1 x_2$

$$\begin{bmatrix} \mathbf{C}\mathbf{V}_1 \mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ \mathbf{0} \\ -x_1 x_2 \mathbf{G} \end{bmatrix} = \begin{bmatrix} \overline{\mathbf{B}} & \\ \underline{\mathbf{B}} & \overline{\mathbf{B}} \\ & \underline{\mathbf{B}} \end{bmatrix} \overbrace{\begin{bmatrix} \mathbf{Z}_1 \mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) \\ x_1 \mathbf{Z}_2 \end{bmatrix}}^{\mathbf{Z}_{12}}$$

next. write $\mathbf{C}\mathbf{V}_1 \mathbf{G}^{-1}(\mathbf{C}\mathbf{V}_2) = \mathbf{C}^{(2)} \cdot \mathbf{V}_{12}$ **[W25]**

$\Rightarrow$ fast verification for deg two polynomials

➋ circuits?

problem. depth d circuits incurs 2^d blow-up

2 circuits?

problem. depth d circuits incurs 2^d blow-up

solution. chainable FC **[BCFL23, GR19]**

❷ circuits?

problem. depth d circuits incurs 2^d blow-up

solution. chainable FC **[BCFL23, GR19]**

open(x, f):

– commit to each layer of the circuit f

– provide openings for adjacent layers

② circuits?

problem. depth d circuits incurs 2^d blow-up

solution. chainable FC **[BCFL23, GR19]**

open(x, f):

– commit to each layer of the circuit f

– provide openings for adjacent layers

new. FC for deg two $f : \{0,1\}^\ell \to \{0,1\}^{\ell_{\text{out}}}$ that

supports opening to **commit**$(f(x))$

3 **compressing** openings

IDEA. Merkle-style recursion [W25,AMR25a]

③ **compressing** openings

base case. $\ell = 2m^2$

3 **compressing** openings

base case. $\ell = 2m^2$

recursion. $\ell/2 \mapsto \ell$

commit$([\mathbf{x}_0 \mid \mathbf{x}_1])$

③ **compressing** openings

base case. $\ell = 2m^2$

recursion. $\ell/2 \mapsto \ell$

commit$([\mathbf{x}_0 \mid \mathbf{x}_1])$

$$\mathbf{C}_0 := \textbf{commit}(\mathbf{x}_0), \mathbf{C}_1 := \textbf{commit}(\mathbf{x}_1) \in \mathbb{Z}_q^{n \times m}$$

③ **compressing** openings

base case. $\ell = 2m^2$

recursion. $\ell/2 \mapsto \ell$

$$\textbf{commit}([\mathbf{x}_0 \mid \mathbf{x}_1])$$

$$\overbrace{\mathsf{bits}(\mathbf{C}_0 \mid \mathbf{C}_1)}^{\in\{0,1\}^{2m^2}}$$

$$\mathbf{C}_0 := \textbf{commit}(\mathbf{x}_0), \mathbf{C}_1 := \textbf{commit}(\mathbf{x}_1) \in \mathbb{Z}_q^{n\times m}$$

❸ **compressing** openings

base case. $\ell = 2m^2$

recursion. $\ell/2 \mapsto \ell$

$$\textbf{commit}([\mathbf{x}_0 \mid \mathbf{x}_1]) :=$$

$$\textbf{commit}(\overbrace{\text{bits}(\mathbf{C}_0 \mid \mathbf{C}_1)}^{\in\{0,1\}^{2m^2}})$$

$$\mathbf{C}_0 := \textbf{commit}(\mathbf{x}_0), \mathbf{C}_1 := \textbf{commit}(\mathbf{x}_1) \in \mathbb{Z}_q^{n\times m}$$

conclusion

FC & SNARGs for P/poly from SIS

conclusion

FC & SNARGs for P/poly from SIS

open problems.

– P without pre-processing

– $|\textbf{proof}| = O(\text{depth}) \mapsto O(1)$

conclusion

FC & SNARGs for P/poly from SIS

open problems.

– P without pre-processing

– $|\textbf{proof}| = O(\text{depth}) \mapsto O(1)$

// merci !