<u>Another view</u>: We can view GSW / homomorphic signatures as homomorphic commitment scheme:

pp: $A \in \mathbb{Z}_q^{n \times m}$

to commit to a message $\mu \in \{0,1\}$, sample $R \xleftarrow{R} D_{\mathbb{Z},s}^{m \times t}$ and output $C \leftarrow AR + \mu \cdot G$

to open a commitment to message $\mu$, reveal $R$ and check that

$$C = AR + \mu \cdot G \quad \text{and} \quad \|R\|_\infty \leq \beta \quad (\text{for some noise bound } \beta)$$

<u>Observe</u>: commitment is just GSW ciphertext, so supports arbitrary computation

$$\begin{aligned} C_1 &= AR_1 + \mu_1 \cdot G \\ &\vdots \qquad \vdots \\ C_\ell &= AR_\ell + \mu_\ell \cdot G \end{aligned} \implies C_f = AR_{f,x} + f(x) \cdot G$$

verifier computes $C_f$ from $C_1, \ldots, C_\ell$

where $R_{f,x} = [R_1 | \cdots | R_\ell] \cdot H_{f,x}$

can be used to open to $f(x)$

Two possible "modes": 1. Suppose $A$ is an LWE matrix: $A = \begin{bmatrix} \bar{A} \\ \bar{s}^T \bar{A} + e^T \end{bmatrix}$.

Then, the commitment scheme is <u>extractable</u>: given trapdoor information, can extract <u>unique</u> message for which an opening exists (if there is such a message).

If $C$ can be opened to $\mu \in \{0,1\}$, then there exists short $R$ such that

$$\begin{aligned} C = AR + \mu \cdot G \implies s^T C &= s^T AR + \mu \cdot s^T G \qquad (s = [-\bar{s} \mid 1]) \\ &= e^T R + \mu \cdot s^T G \\ &\approx \mu \cdot s^T G \quad \text{which suffices to recover } \mu \end{aligned}$$

Extractable commitment $\implies$ statistically binding

2. Suppose $A$ is random matrix: $A \xleftarrow{R} \mathbb{Z}_q^{n \times m}$

Then, the commitment scheme is <u>equivocable</u>: given trapdoor information, can open a commitment to <u>both</u> 0 or 1.

To see this, sample $(A, T) \leftarrow \text{TrapGen}(n, q)$. Then $A$ is statistically close to uniform.

To generate opening for commitment $C$ to message $\mu \in \{0,1\}$,

$$R \leftarrow \text{SamplePre}(A, T, C - \mu G, s)$$

This yields short $R$ where

$$AR = C - \mu G \implies C = AR + \mu \cdot G$$

Equivocable commitment $\implies$ statistically hiding

What if we want hiding + binding? Cannot get statistical for both, but can get statistical for one property and computational for the other.

<u>Dual-mode commitment</u>: public parameters can be generated in two different modes

1) Statistical binding mode
2) Statistical hiding mode

parameters for two modes <u>computationally</u> indistinguishable

$\implies$ statistically binding, computationally hiding

statistically hiding, computationally binding

follows by simple hybrid argument

<u>Example</u>: Computational binding in equivocable mode:

<u>$\text{Hyb}_0$</u>: adversary given pp as sampled in equivocable mode

<u>$\text{Hyb}_1$</u>: adversary given pp as sampled in extractable mode

adversary's advantage changes by a negligible amount (indistinguishability of pp)

advantage of adversary is negl. (statistical binding)

Above commitment scheme is dual mode (under LWE).

Application to (designated-prover) NIZK for NP language $\mathcal{L}$ (let $\mathcal{R}$ be associated relation)

$$(vk, sk) \leftarrow \mathsf{Setup}(1^\lambda)$$

$sk \downarrow$ prover $(x, w)$ $\qquad\qquad$ $vk \downarrow$ verifier $(x)$

$$\xrightarrow{\quad \pi \quad}$$

<u>Requirements</u>:

1) <u>Completeness</u>: if $x \in \mathcal{L}$, then $\mathsf{Verify}(vk, x, \pi) = 1$
2) <u>Soundness</u>: if $x \notin \mathcal{L}$, then $\mathsf{Verify}(vk, x, \pi) = 1$ with prob. $\mathsf{negl}(\lambda)$
3) <u>Multi-theorem ZK</u>: <u>same</u> proving key $sk$ can be used to construct <u>multiple</u> proofs and still preserve ZK

↳ For every efficient adversary $\mathcal{A}$, there exists an efficient simulator $\mathcal{S} = (\mathcal{S}_0, \mathcal{S}_1)$ such that $(vk, sk) \leftarrow \mathsf{Setup}(1^\lambda)$, $(\widetilde{vk}, \widetilde{st}) \leftarrow \mathcal{S}_0(1^\lambda)$:

$$\left| \Pr\left[\mathcal{A}^{\mathcal{O}_0(sk,\cdot,\cdot)}(vk) = 1\right] - \Pr\left[\mathcal{A}^{\mathcal{O}_1(\widetilde{st},\cdot,\cdot)}(\widetilde{vk}) = 1\right] \right| = \mathsf{negl}(\lambda)$$

where $\mathcal{O}_0(sk, x, w)$ outputs $\mathsf{Prove}(sk, x, w)$ if $\mathcal{R}(x, w) = 1$ and $\perp$ otherwise

$\mathcal{O}_1(\widetilde{st}, x, w)$ outputs $\mathcal{S}_1(\widetilde{st}, x, w)$ if $\mathcal{R}(x, w) = 1$ and $\perp$ otherwise

<u>Attempt 1</u>: Commit to witness $w$, homomorphically evaluate $\mathcal{R}(x, \cdot)$ on $w$ and open output to $1 = \mathcal{R}(x, w)$

$pp \leftarrow \mathsf{Setup}(1^\lambda)$ (to prover and verifier)

<u>prover</u> $(x, w)$ $\qquad\qquad$ <u>verifier</u> $(x)$

$\sigma_w \leftarrow \mathsf{Commit}(pp, w)$

$\sigma_{\mathcal{R}(x,w)} \leftarrow \mathsf{Eval}(pp, \sigma, \mathcal{R}(x, \cdot))$

$\tau \leftarrow \mathsf{Open}(pp, \sigma_{\mathcal{R}(x,w)}, 1)$

$$\xrightarrow{\quad \sigma_w,\ \tau \quad}$$

compute $\mathcal{R}(x, \cdot)$ on $\sigma_w$ to obtain $\sigma_{\mathcal{R}(x,w)}$

check that $\sigma_{\mathcal{R}(x,w)}$ opens to $1$ (using $\tau$)

Zero-knowledge holds if commitment scheme is context-hiding

Soundness is problematic: binding/unforgeability assumes that initial commitment $(\sigma_w)$ is honestly generated — but may not be the case!

<u>Attempt 2</u>: Move commitment to the public parameters

$pp \leftarrow \mathsf{Setup}(1^\lambda)$

$\sigma_w \leftarrow \mathsf{Commit}(pp, w)$

(to prover and verifier)

prover also given commitment randomness associated with $\sigma_w$ (to allow computing openings)

<u>prover</u> $(x, w)$ $\qquad\qquad$ <u>verifier</u> $(x)$

$\sigma_{\mathcal{R}(x,w)} \leftarrow \mathsf{Eval}(pp, \sigma, \mathcal{R}(x, \cdot))$

$\tau \leftarrow \mathsf{Open}(pp, \sigma_{\mathcal{R}(x,w)}, 1)$

$$\xrightarrow{\quad \sigma_w,\ \tau \quad}$$

compute $\mathcal{R}(x, \cdot)$ on $\sigma_w$ to obtain $\sigma_{\mathcal{R}(x,w)}$

check that $\sigma_{\mathcal{R}(x,w)}$ opens to $1$ (using $\tau$)

<u>Problem</u>: Public parameters now depends on <u>witness</u>!

Scheme does not support proving general relations.

Zero-knowledge not affected (by context-hiding + hiding)

soundness follows from binding/unforgeability

<u>Solution</u>: Add layer of indirection.

<u>Setup</u>: Sample a key $k$ for a symmetric encryption scheme
Sample parameters pp for commitment scheme and construct commitment $\sigma$ to $k$ with randomness $r$

Secret (proving) key: $sk = (k, r)$
Public (verification) key: $vk : \sigma$

circuit <u>only</u> depends on statement $x$ and ciphertext ct (<u>known</u> to verifier)

Decrypt ciphertext and apply NP relation

$\text{Prove}(\underset{=(k,r)}{sk}, x, w)$: $ct \leftarrow \text{Encrypt}(k, w)$
Define the circuit $C_{x,ct}(k) := R(x, \text{Decrypt}(k, ct))$
Homomorphically evaluate $C_{x,ct}$ on $\sigma$ and compute an opening $\tau_{x,ct}$ to the bit 1:
$\pi \leftarrow (ct, \tau_{x,ct})$

$\text{Verify}(\underset{=\sigma}{vk}, x, \underset{=(ct,\tau_{x,ct})}{\pi})$: Homomorphically evaluate $C_{x,ct}$ on $\sigma$ and check that $\tau_{x,ct}$ is an opening to 1 w.r.t. $C_{x,ct}$ and $\sigma$

<u>Soundness</u>: Follows by binding / unforgeability property of commitment.
In particular, if $x \notin \mathcal{L}$, then $C_{x,ct}(k) = 0$ for <u>all</u> ciphertexts.
Prover that can open $\sigma$ (commitment on $k$) to 1 under $C_{x,ct}$ breaks binding / unforgeability.

If scheme is statistically binding, then construction is statistically sound.

<u>Zero-knowledge</u>: For a true statement, commitment always opens to 1. Can use context-hiding / equivocation to simulate.
$S_0(1^\lambda)$: Sample $k \xleftarrow{R} \mathcal{K}$ (key-space of symmetric encryption scheme)
Sample public parameters pp and an equivocation trapdoor td for the commitment scheme
↳ for the lattice-based scheme, this is a trapdoor for $A \in \mathbb{Z}_q^{n \times m}$ (where $A$ is the public parameters)
Construct a commitment $\sigma$ to the secret key $k$
Output $\widetilde{vk} = (pp, \sigma)$ and $\widetilde{st} = (k, td)$

$S_1(\underset{=(k,td)}{\widetilde{st}}, x)$: Compute $ct \leftarrow \text{Encrypt}(k, 0^{|w|})$.
Use td to sample an opening $\tau$ to 1 w.r.t. $C_{x,ct}$
Output $(ct, \tau)$

Simulated verification key is computationally (or statistically) indistinguishable from real verification key
Real ciphertext computationally indistinguishable from simulated ciphertexts by CPA security
Real openings are statistically indistinguishable from simulated openings by context-hiding / equivocation
↳ in equivocation mode

<u>Summary</u>: designated-prover NIZK from context-hiding homomorphic commitments