

Another view: 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 $R \leftarrow \mathbb{Z}_{2,5}^{m \times t}$ and output $C \leftarrow AR + \mu \cdot G$

to open a commitment to message μ , reveal R and check that

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

Observe: commitment is just GSW ciphertext, so supports arbitrary computation

$$C_1 = AR_1 + \mu_1 \cdot G$$

\vdots

$$C_\ell = AR_\ell + \mu_\ell \cdot G$$

$$\Rightarrow C_f = AR_{f,x} + f(x) \cdot G$$

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

verifier computes

C_f from C_1, \dots, C_ℓ

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

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

Then, the commitment scheme is extractable: given trapdoor information, can extract unique 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

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

Extractable commitment \Rightarrow statistically binding

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

Then, the commitment scheme is equivocal: given trapdoor information, can open a commitment to both 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

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

Equivocal commitment \Rightarrow 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.

Dual-mode commitment: public parameters can be generated in two different modes

1) Statistical binding mode

2) Statistical hiding mode

parameters for two modes computationally indistinguishable

\Rightarrow statistically binding, computationally hiding
statistically hiding, computationally binding

follows by simple hybrid argument

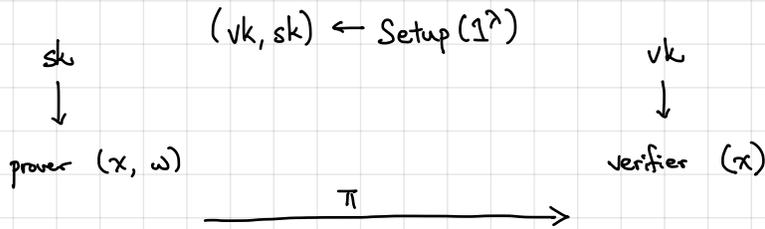
Example: Computational binding in equivocal mode:

adversary's advantage changes by a negligible amount (indistinguishability of pp) \rightarrow Hyb₀: adversary given pp as sampled in equivocal mode
Hyb₁: adversary given pp as sampled in extractable mode

\rightarrow 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 R be associated relation)

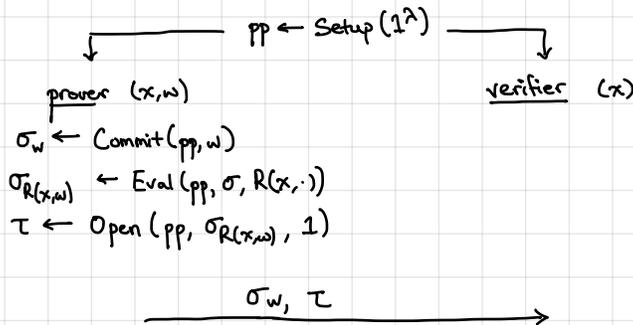


- Requirements:
- 1) Completeness: if $x \in \mathcal{L}$, then $\text{Verify}(vk, x, \pi) = 1$
 - 2) Soundness: if $x \notin \mathcal{L}$, then $\text{Verify}(vk, x, \pi) = 1$ with prob. $\text{negl}(\lambda)$
 - 3) Multi-theorem ZK: same proving key sk can be used to construct multiple proofs and still preserve ZK
 ↳ For every efficient adversary A , there exists an efficient simulator $S = (S_0, S_1)$ such that
 $(vk, sk) \leftarrow \text{Setup}(1^\lambda), (\tilde{vk}, \tilde{sk}) \leftarrow S_0(1^\lambda)$:

$$\left| \Pr[A^{O_0(sk, \cdot, \cdot)}(vk) = 1] - \Pr[A^{O_1(\tilde{sk}, \cdot, \cdot)}(\tilde{vk}) = 1] \right| = \text{negl}(\lambda)$$

where $O_0(sk, x, w)$ outputs $\text{Prove}(sk, x, w)$ if $R(x, w) = 1$ and \perp otherwise
 $O_1(\tilde{sk}, x, w)$ outputs $S_1(\tilde{sk}, x, w)$ if $R(x, w) = 1$ and \perp otherwise

Attempt 1: Commit to witness w , homomorphically evaluate $R(x, \cdot)$ on w and open output to $1 = R(x, w)$

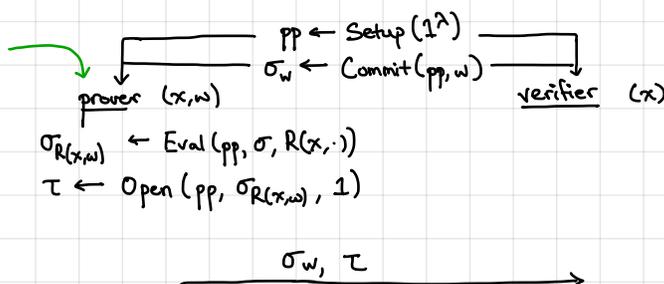


compute $R(x, \cdot)$ on σ_w to obtain $\sigma_{R(x, w)}$
 check that $\sigma_{R(x, w)}$ opens to 1 (using τ)

Zero-knowledge holds if commitment scheme is context-hiding
 Soundness is problematic: binding/unforgeability assumes that initial commitment (σ_w) is honestly generated — but may not be the case!

Attempt 2: Move commitment to the public parameters

prover also given commitment randomness associated with σ_w (to allow computing openings)



compute $R(x, \cdot)$ on σ_w to obtain $\sigma_{R(x, w)}$
 check that $\sigma_{R(x, w)}$ opens to 1 (using τ)

Problem: Public parameters now depends on witness!
 Scheme does not support proving general relations.

Zero-knowledge not affected (by context-hiding + hiding)
 soundness follows from binding/unforgeability

Solution: Add layer of indirection.

Setup: Sample a key k for a symmetric encryption scheme
Sample parameters pp for commitment scheme and construct commitment σ to k with randomness r

Secret (proving) key: $sk = (k, r)$

Public (verification) key: $vk = \sigma$

circuit only depends on statement x and ciphertext ct
(known to verifier)

Prove (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 σ and compute an opening $\tau_{x,ct}$ to the bit 1:

$\pi \leftarrow (ct, \tau_{x,ct})$

Decrypt ciphertext and apply NP relation

Verify (vk, x, π) :

Homomorphically evaluate $C_{x,ct}$ on σ and check that $\tau_{x,ct}$ is an opening to 1 w.r.t. $C_{x,ct}$ and σ

Soundness: Follows by binding/unforgeability property of commitment.

In particular, if $x \notin L$, then $C_{x,ct}(k) = 0$ for all ciphertexts.

Prover that can open σ (commitment on k) to 1 under $C_{x,ct}$ breaks binding/unforgeability.

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

Zero-knowledge: For a true statement, commitment always opens to 1. Can use context-hiding/equivocation to simulate.

$S_0(\mathbb{1}^x)$: Sample $k \xleftarrow{R} K$ (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 σ to the secret key k

Output $\tilde{vk} = (pp, \sigma)$ and $\tilde{sk} = (k, td)$

$S_1(\tilde{sk}, x)$: Compute $ct \leftarrow \text{Encrypt}(k, 0^{|w|})$.

Use td to sample an opening τ to 1 w.r.t. $C_{x,ct}$

Output (ct, τ)

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

Summary: designated-prover NIZK from homomorphic commitments
context-hiding