A New Approach for Non-Interactive Zero Knowledge from Learning with Errors

Brent Waters

NTT Research

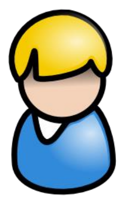
THE UNIVERSITY OF TEXAS AT AUSTIN

Non-Interactive Zero Knowledge Proofs (NIZKs) [Goldwasser-Micali-Rackoff85, Blum-Feldman-Micali88]

CRS

Statement : $x \in \{0,1\}^n$

Witness : $w \in \{0,1\}^h$



CRS

Statement : $x \in \{0,1\}^n$

$\text{Prove}(\text{CRS}, x, w) \rightarrow \pi$

$\text{Verify}(\text{CRS}, x, \pi)$

Sound: Only accepts if exists w where R(x,w) =1

Zero Knowledge: Verifier learns no information about witness w

Hidden Bits Approach to NIZKs [Feige-Lapidot-Shamir90]

Part 1: Build NIZKs from “hidden bits model”

- Random string chosen
- Prover can reveal, but not change

1	0	1	1	0	0	0	1	0	1	0

Part 2: Build Hidden Bits Generators

- Small commitment com to arbitrary k number of bits
- Com is statistically binding for all outputs
- Unopened bits computationally hidden

NIZKs from Number Theory

1990 QR [BFM88]; RSA via hidden bits [FLS90]

2000

Bilinear maps via hidden bits [CHK03]

Learning with Errors (LWE) introduced by Regev05

Bilinear maps directly gate by gate[GOS06]

2010

LWE: Fully Homomorphic encryption, IBE, ABE…
<u>But no NIZKs!</u>

LWE via correlation intractability [CCHLRRW19, PS19]

2020

But why didn't hidden bits model work?

Why ask why?

Understanding: Fundamental barrier? Or not approaching the right way?

Techniques: Hope to solve other problems

Efficiency: Black box use of underlying cryptography

Result: New hidden bits realization of NIZK from LWE

Hidden Bits Generator

Setup$(1^{\lambda},\ 1^{k}) \rightarrow$ crs

GenBits(crs) $\rightarrow$ com, $(r_1, \ldots, r_k), (\pi_1, \ldots, \pi_k)$

Verify(crs, com, $i, \beta, \pi) \rightarrow\ b \in \{0,1\}$

Succinctness: $|\text{com}| = \text{poly}(\lambda)$ $\quad\quad$ $(\mathit{independent\ of\ } k)$

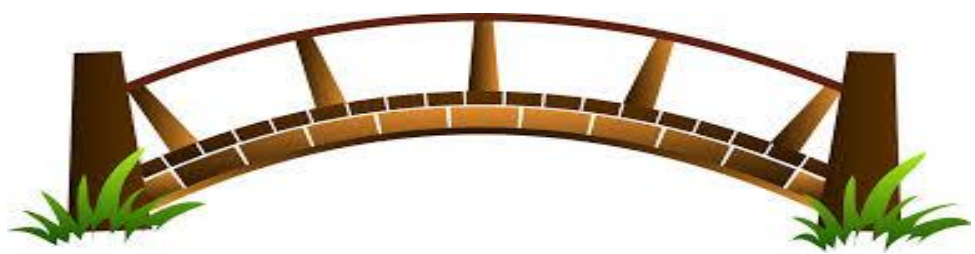
Binding: $\forall \quad i \quad \nexists$ (com, π^0, π^1) s.t.
Verify(crs,com, $i, 0, \pi^0) = 1$ AND Verify(crs,com, $i, 1, \pi^1$)

Hiding: $\forall i$ Att cannot distinguish r_i from random given
$(crs, com, \{\pi_j, r_j\}_{j \neq i})$

Dual Mode Setup

LWE: $A, \boldsymbol{s}A + noise \ \approx_c \ A, U$

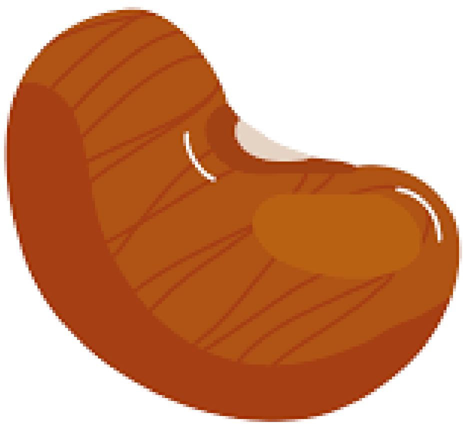
Binding Mode



Hiding Mode

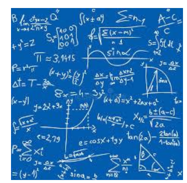
Design Principles

Seed



>

Bits + Proofs



>

Commitment

Succinctness: Small commitment

Binding: Structured CRS component 

Hiding: Big seed + random CRS component

Binding Mode

Construction Binding Mode

Setup$(1^\lambda, 1^k) \rightarrow$ crs

(1) Choose prime $q \approx 2^\lambda$,

Params: $n < m = 2\lg(q)\, n < \quad L = \lambda m k$

Com length

Seed length

(2) $U \overset{R}{\leftarrow} \mathrm{Z}_{\mathrm{q}}^{\mathrm{n} \times L}$

Using TrapGen/SamplePre GPV09

(3) Sample $A_i \in Z_q^{n \times m}$ $\mathrm{W_i} \in Z_q^{m \times L}$: $U = A_i W_i$; W_i short $\quad i \in [k]$

(4) For $i \in [k]$ $\quad \mathbf{s}_\mathrm{i} \overset{R}{\leftarrow} \mathrm{Z}_\mathrm{q}^\mathrm{n}$, $\quad \mathbf{e}_\mathrm{i} \overset{R}{\leftarrow} D_\sigma^m$ $\quad \mathrm{v}_i = \boldsymbol{s}_i^T\, \mathrm{A_i} + \mathbf{e}_\mathrm{i}^T$

Construction (continued)

GenBits(crs)

(1) $\boldsymbol{t} \stackrel{R}{\leftarrow} \left[-2^{.5\,\lambda}, 2^{.5\,\lambda}\right]^L$

(2) $\text{com} = U\,\boldsymbol{t} \in Z_q^n$

(3) $\boldsymbol{\pi}_i = W_i\,\boldsymbol{t}, \qquad r_i = \lfloor \boldsymbol{v}_i^T\,\boldsymbol{\pi}_i \rceil$

Verify(crs, com, $i, \beta, \boldsymbol{\pi}$)

(1) Check $\quad \text{com} = A_i\boldsymbol{\pi} \quad$ AND $\quad \lfloor \boldsymbol{v}_i^T \boldsymbol{\pi}_i \rceil = \beta$

(2) Check $\left|\left|\boldsymbol{\pi}_i\right|\right|_\infty \leq 2^{\lambda^{.6}}$

Correctness: $A_i\,\boldsymbol{\pi}_i \quad = \quad A_i\,W_i\,\boldsymbol{t} \;=\; U\,\boldsymbol{t} = \;\text{com}$

$\boldsymbol{\pi}_i = W_i\,\boldsymbol{t}, \qquad U = A_i W_i$

Over Simplified Binding Analysis

Imagine: $\mathrm{v}_i = \mathbf{s}_\mathrm{i}^T \mathrm{A}_\mathrm{i} + \mathbf{e}_\mathrm{i}^T$

Proof verification $\Longrightarrow$ $A_i \, \boldsymbol{\pi}_i = \mathrm{com}$

$$r_i = \lceil \boldsymbol{v}_i \boldsymbol{\pi}_i \rfloor$$

$$= \lceil (\boldsymbol{s}_i^T A_i) \boldsymbol{\pi}_i \rfloor \qquad \text{(imagined binding mode setup)}$$

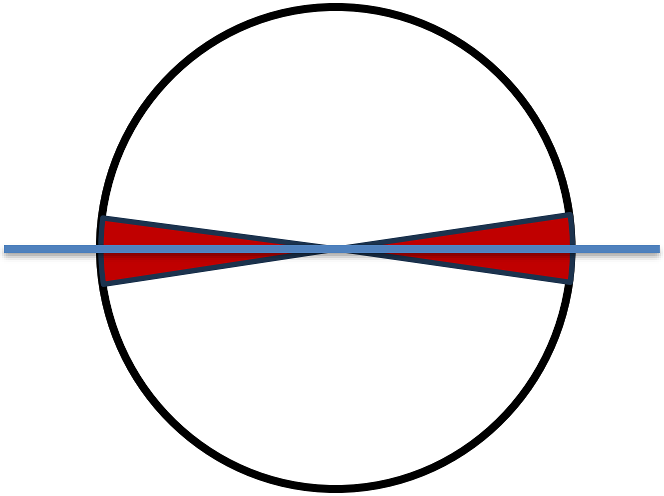
$$= \lceil \boldsymbol{s}_i^T \mathrm{com} \rfloor \qquad \text{(proof verifies)}$$

Takeaway: Bit completely determined by com and parameters!

Actual Binding Analysis

Reality: $v_i = \mathbf{s}_i^T A_i + \mathbf{e}_i^T$

$r_i = \lfloor \boldsymbol{s}_i^T \text{com} + \boldsymbol{e}_i^T \boldsymbol{\pi}_i \rceil$ $< 2^{\lambda^{.7}}$



Issue: Different $\boldsymbol{\pi}_i$ could lead to different bits!

Solution: Reject dangerous cases

Verify$(\text{crs}, \text{com}, i, \beta, \boldsymbol{\pi})$

(1) Check $\text{com} = A_i \boldsymbol{\pi}$ AND $\lfloor \boldsymbol{v}_i^T \boldsymbol{\pi}_i \rceil = \beta$

(2) Check $||\boldsymbol{\pi}_i||_\infty \leq 2^{\lambda^{.6}}$

(3) Reject if $\boldsymbol{v}_i^T \boldsymbol{\pi}_i$ within $2^{\lambda^{.7}}$ of rounding boundary

Options: Negligible correctness error OR push to hiding error

Hiding Mode

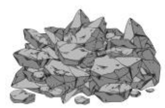
Construction Hiding Mode

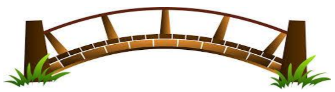
Setup$(1^\lambda, 1^k) \rightarrow$ crs

(1) Choose prime $q \approx 2^\lambda$, params $n < m = 2\lg(q)\, n < L = \lambda mk$

(2) $U \xleftarrow{R} \mathrm{Z}_\mathrm{q}^{\mathrm{n}\times L}$

(3) Sample $A_i \in Z_q^{n \times m}$ $\mathrm{W_i} \in Z_q^{m\times L}$: $U = A_i W_i$; W_i short $i \in [k]$

(4) $\mathbf{v}_\mathrm{i} \xleftarrow{R} \mathrm{Z}_\mathrm{q}^\mathrm{m}$ $i \in [k]$ 



Bridging Modes via LWE

$$A_i, \mathbf{v}_i = \mathbf{s}_i^T A_i + \mathbf{e}_i^T \quad \text{vs} \quad A_i, \mathbf{v}_i \xleftarrow{R} \mathrm{Z}_q^m$$

Immediately from LWE?

Params: $U = A_i W_i$; W_i short $\quad i \in [k]$

Issue: Reduction needs trapdoors for ~~all~~ A_i

Solution: Reduction needs trapdoor for all but one A_i

Hybrid Proof

Hybrid j: $\mathbf{v}_\mathrm{i} = \mathbf{s}_\mathrm{i}^T \mathrm{A}_\mathrm{i} + \mathbf{e}_\mathrm{i}^T \quad \mathrm{i} \in [\mathrm{j}, \mathrm{k}]$

$\mathbf{v}_\mathrm{i} \overset{R}{\leftarrow} \mathrm{Z}_\mathrm{q}^\mathrm{m} \qquad \mathrm{i} \in [1, j-1]$

Indistinguishability of Hyb j-1 and Hyb j:

Reduction gets A_j from LWE challenger samples other A_i itself

Hiding Analysis of i-th bit

Lynchpin:

$\exists$ short $\boldsymbol{c}$:

(A) $W_j\, \boldsymbol{c} = 0^m \quad \forall j \neq i$ Does not change proofs

(B) $\boldsymbol{v}_i^T\, W_i \boldsymbol{c} = \lfloor \frac{q}{2} \rceil$ Flips ith bit

Goals:

(1) Show vector exists

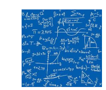
(2) Show it hides ith bit

Establishing the vector

$\exists$ short $\boldsymbol{c}$: $\quad W_j\, \boldsymbol{c} = 0^m \qquad \forall j \neq i$ AND $\boldsymbol{v}_i^T\, W_i \boldsymbol{c} = \lfloor \frac{q}{2} \rfloor$

$\exists\ \boldsymbol{y} \neq \boldsymbol{z} \in \{0,1\}^L : \ W_j\, \boldsymbol{y} = W_j\, \boldsymbol{z} \quad \forall\, j \neq i$

$\boldsymbol{h} = \ \boldsymbol{y} - \boldsymbol{z} \in \{-1,0,1\}$: $\ W_j\, \boldsymbol{h} = 0^m \quad \forall\, j \neq i$

 $>$ 

Collect: Linearly independent $\boldsymbol{h}_1, \dots, \boldsymbol{h}_T$: $\ W_j\ h_k = 0^m$

W.h.p. exists: $x_1, \dots, x_T \in \{0,1\} : \boldsymbol{v}_i^T\ W_i(x_1 \boldsymbol{h}_1 + \cdots x_T \boldsymbol{h}_T) = \lfloor \frac{q}{2} \rfloor$

Leftover hash lemma & randomness of v 

Bit hiding with smudging

$\text{GenBits}_0(\text{ crs })$

(1) $\boldsymbol{t} \overset{R}{\leftarrow} [-2^{.5\lambda}, 2^{.5\lambda}]$

(2) $\text{com} = U(\boldsymbol{t})$

(3) $\boldsymbol{\pi}_j = W_j(\boldsymbol{t}), \qquad r_j = \lfloor \boldsymbol{v}_j^T W_j(\boldsymbol{t}) \rceil$

$\text{GenBits}_1(\text{ crs })$

(1) $\boldsymbol{t} \overset{R}{\leftarrow} [-2^{.5\lambda}, 2^{.5\lambda}]$, $b \overset{R}{\leftarrow} \{0,1\}$

(2) $\text{com} = U(\boldsymbol{t} + b\boldsymbol{c})$

(3) $\boldsymbol{\pi}_j = W_j(\boldsymbol{t} + b\boldsymbol{c}), \qquad r_j = \lfloor \boldsymbol{v}_j^T W_j(\boldsymbol{t} + b\boldsymbol{c}) \rceil$

Indistinguishable due to size of **t** relative to **c**

Attackers advantage negligibly close

Bit flipping

GenBits$_1$(crs)

(1) $\boldsymbol{t} \xleftarrow{R} \left[-2^{.5\,\lambda}, 2^{.5\,\lambda}\right], b \xleftarrow{R} \{0,1\}$

(2) $\text{com} = U\,(\boldsymbol{t} + b\boldsymbol{c})$

(3) $\boldsymbol{\pi}_j = W_j\,(\boldsymbol{t} + b\boldsymbol{c}),\qquad r_j = \lfloor\, \boldsymbol{v}_j^T\, W_j(\boldsymbol{t} + b\boldsymbol{c})\,\rceil$

GenBits$_2$(crs)

(1) $\boldsymbol{t} \xleftarrow{R} \left[-2^{.5\,\lambda}, 2^{.5\,\lambda}\right], b \xleftarrow{R} \{0,1\}$

(2) $\text{com} = U\,(\boldsymbol{t})$

(3) $\boldsymbol{\pi}_j = W_j\,(\boldsymbol{t}),\qquad r_j = \left\lfloor \boldsymbol{v}_j^T\, W_j(\boldsymbol{t})\right\rceil \qquad \forall j \neq i$

(4) $r_i = \left\lfloor \boldsymbol{v}_i^T\, W_i(\boldsymbol{t})\right\rceil \oplus b$

(A) $W_j\,\boldsymbol{c} = 0^m \quad \forall j \neq i, U\boldsymbol{c} = 0^n$

(B) $\boldsymbol{v}_i^T\, W_i\boldsymbol{c} = \lfloor\frac{q}{2}\rceil$

No Information!

GenBits$_2$(crs)

(1) $\boldsymbol{t} \xleftarrow{R} \left[-2^{.5\,\lambda}, 2^{.5\,\lambda}\right], b \xleftarrow{R} \{0,1\}$

(2) $\text{com} = U\,(\boldsymbol{t})$

(3) $\boldsymbol{\pi}_j = W_j\,(\boldsymbol{t}),\qquad r_j = \lfloor \boldsymbol{v}_j^T\, W_j(\boldsymbol{t}) \rceil \qquad \forall j \neq i$

(4) $r_i = \lfloor \boldsymbol{v}_i^T\, W_i(\boldsymbol{t}) \rceil \oplus b$

Bilinear Maps to LWE

Target Group Assumption:

$g^{a}, g^{b}, g^{c}, e(g,g)^{\{abc\}} \approx_c g^{a}, g^{b}, g^{c}, h$

Source Group Assumption:

$g^{a}, g^{b}, g^{c}, g^{\{abc\}} \approx_c g^{a}, g^{b}, g^{c}, u$

Bilinear Maps to LWE

Target Group Assumption

- Adaptive IBE
- Selective Attribute-Based Encryption
- Hidden Bits NIZK

Source Group Assumption

- Adaptive ABE
- Broadcast Encryption w/o q-type
- GOS style NIZK

Followup Work

W-Wee-Wu:

LWE NIZK: (A) transparent setup, (B)poly-size modulus, (C) Short CRS

Branco-Choudhuri-Döttling-Jain-Malavota-Srinivasan:

LWE NIZK: (A) transparent setup, (B) poly-size modulus

DDH+LPN NIZK

Bradley-Lu-Nassar-W-Wu:

LWE ZAP

Conclusions and Thoughts

Hidden bits model works for LWE

Retrospective: RSA solution --- CRS publishes images, prover publishes short function + inverses of images

Our Solution: Joint sampling of small commitment


Q&A