Lattice-based Σ-protocols

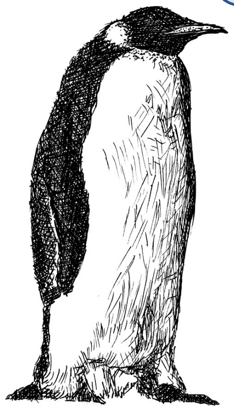
Lisa Kohl

Cryptology Group, CWI Amsterdam

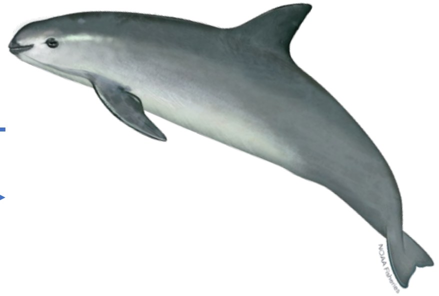
Foundations and Applications of Zero-Knowledge Proofs, Edinburgh

Post-quantum zero knowledge proofs

I know witness w
for statement X

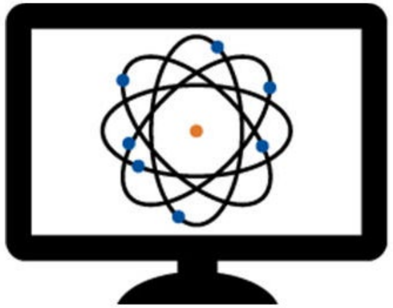


Prover



Verifier (Vaquita)

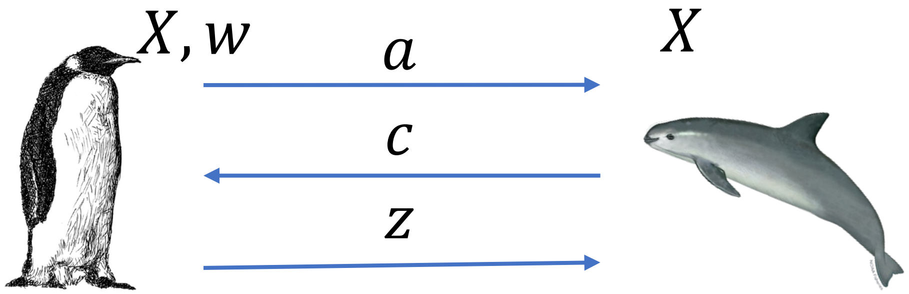
- **This talk:** What if DLOG is no longer hard?
- **Issue:** Soundness does no longer hold!



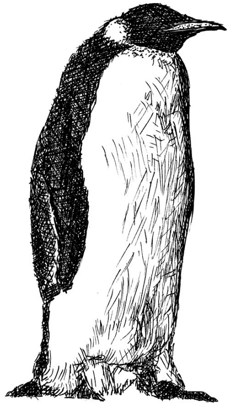
Here we focus on soundness & ZK, but these can also be compressed! [AttemaCramer**Kohl**’ 21]

Application: Digital signatures

Application: Post-quantum signatures



$$pk = X$$



From Sigma-Protocols to Signatures [Schnorr signatures]:

$Sign(pk, m)$:

- Choose/ compute 'commitment' a
- Compute $c = H(pk, a, m)$
- *Compute third-round message z*
- Output signature $\sigma = (a, z)$

(H *modeled as a random oracle)*

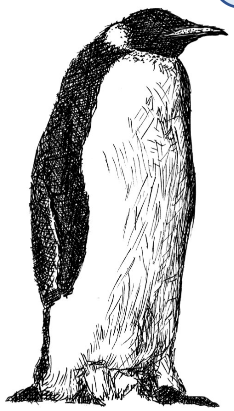
Post-quantum signatures:
e.g.,
- [Lyubashevsky'09,'11]
- CRYSTALS-Dilithium

I know witness w
for statement X

Recall: Σ-protocols

Recall: Σ-protocols

I know witness w
for statement X

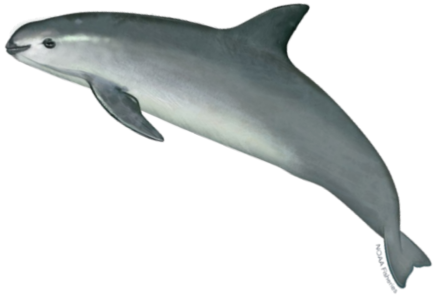


Prover

a →

c ← $c \xleftarrow{\$} \mathcal{C}$

z → $b \in \{0,1\}$

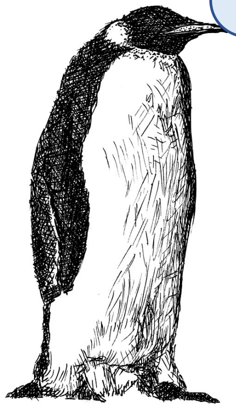


Verifier (Vaquita)

- Σ-protocols satisfy:
  - **Perfect completeness:** Every honest transcript is accepting (i.e., V outputs 1)
  - **(2-)Special soundness:** Giving two accepting transcripts $(a, c, z), (a, c', z')$ with $c \neq c'$ one can efficiently compute a witness $\tilde{w}$ for X
  - **Honest verifier zero knowledge:** Honest transcripts can be efficiently simulated (without knowing the witness w)

We already have a blue-print!

I know value $\vec{w}$
such that $\boxed{\vec{w}}$
can be opened to $\vec{w}$



Prover

$\vec{r} \leftarrow \mathbb{Z}_q^m$

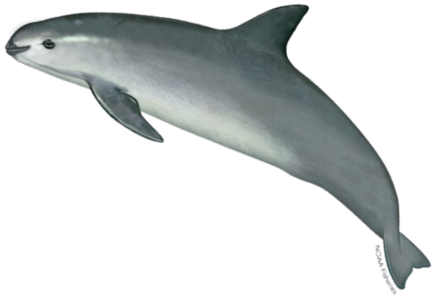
$\boxed{\vec{r}}$

c

$c \leftarrow \mathbb{Z}_q$

$\vec{z} = \vec{r} + c \cdot \vec{w}$

$\boxed{\vec{w}}$



Verifier (Vaquita)

$\boxed{\vec{z}} \overset{?}{=} \boxed{\vec{r}} + c \cdot \boxed{\vec{w}}$

Have to instantiate the commitment scheme from a new assumption!

Instantiating Σ-protocols from lattices

Homomorphic commitments

Commitment scheme: Commit to w via $\boxed{w}$ such that:

- **Hiding:** $\boxed{w}$ hides w
- **Binding:** $\boxed{w}$ can only be opened to x

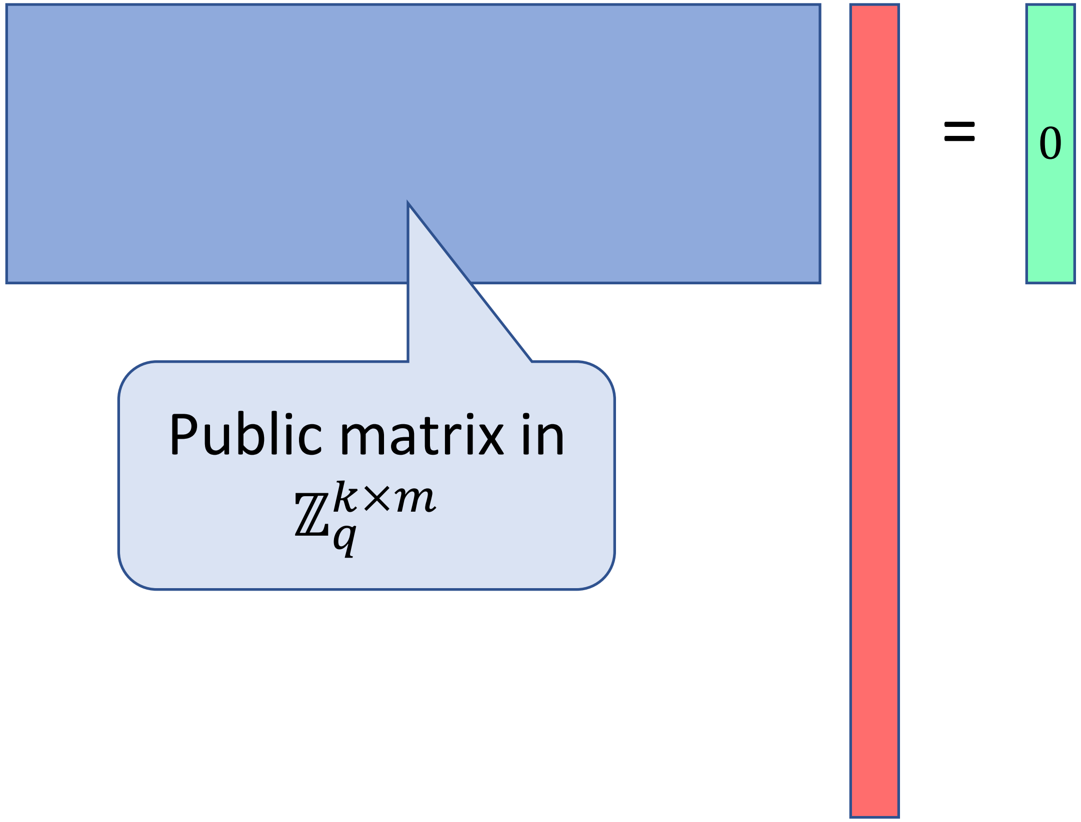
Additional required properties:

- **Homomorphic:** $\boxed{w} + \boxed{v} = \boxed{w+v}$
- **(Succinct:)** $|\boxed{w}| \ll |w|$

Short Integer Solution (SIS)

Here: consider infinity norm $||\vec{s}|| := \max_i |s_i|$

- **SIS Assumption:** It is difficult to find non-zero **short integer solution** $s \in \mathbb{Z}_q^m$ with $||\vec{s}|| \leq b$ and $A \cdot \vec{s} = 0 \bmod q$



Note: Easy to solve without $||\vec{s}|| < b$

Public matrix in $\mathbb{Z}_q^{k \times m}$

Believed to be hard to solve even with a quantum computer

Homomorphic Commitments from MSIS

$\vec{w}$ =

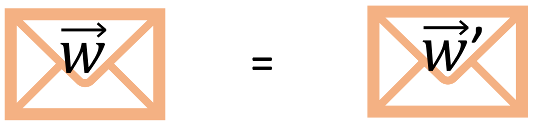
Public matrix in $\mathbb{Z}_q^{k \times m}$

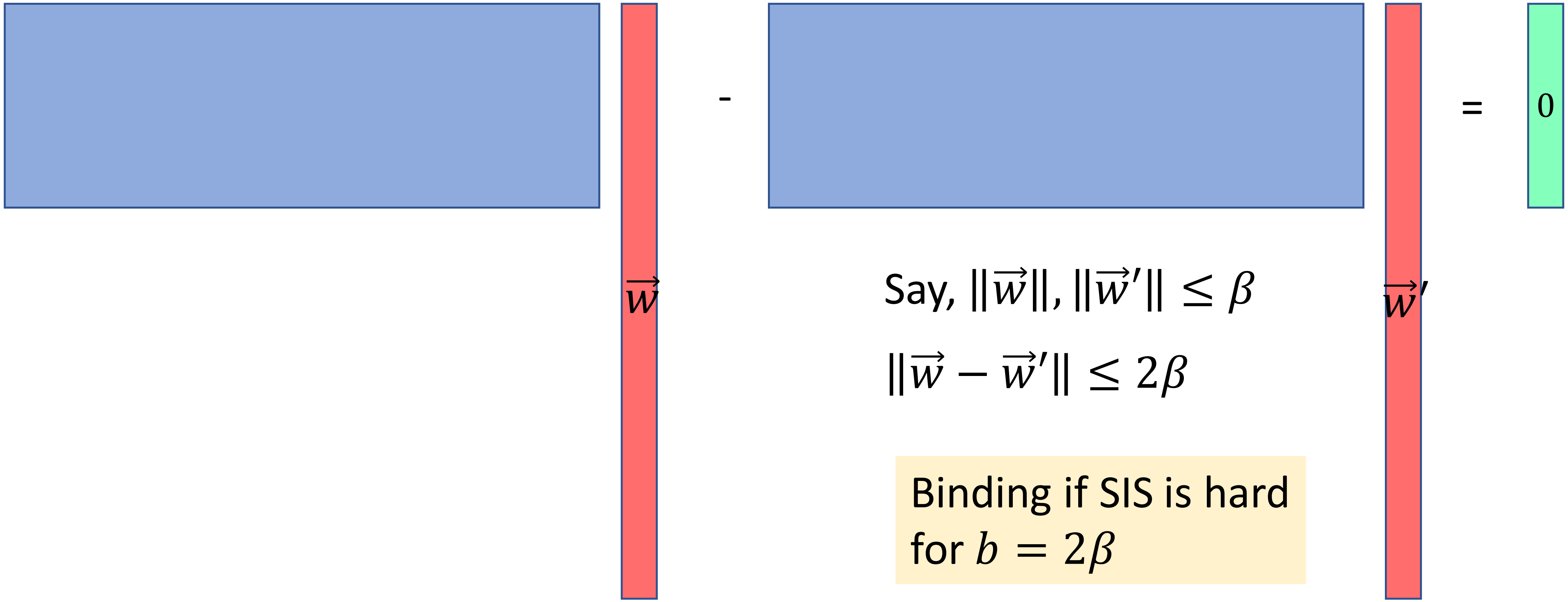
$\vec{w}$

Has to be small, e.g., in binary representation

- **Hiding:** ✓ (when adding some randomness)
- **Binding:**

Binding



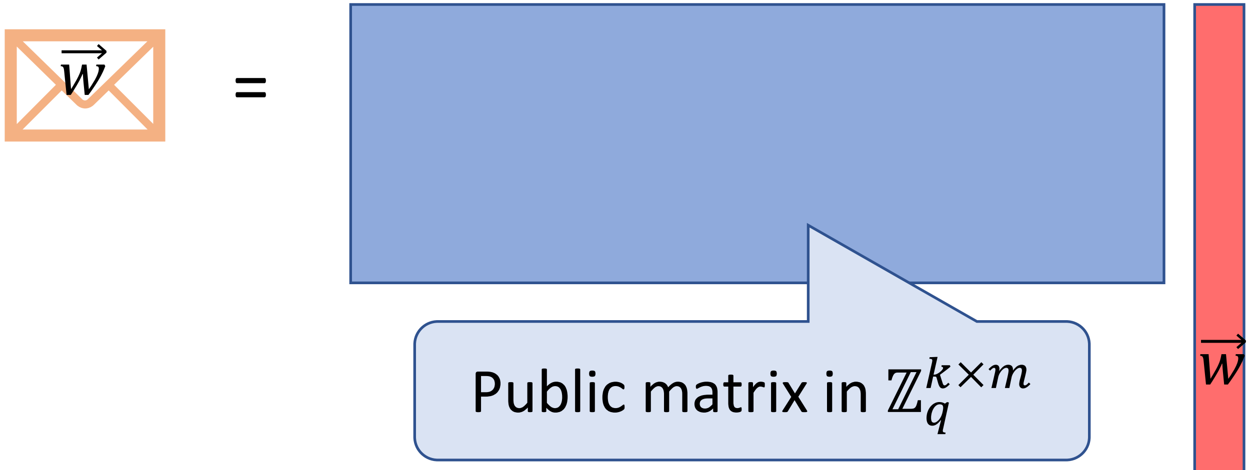


Say, $\|\vec{w}\|, \|\vec{w}'\| \leq \beta$

$\|\vec{w} - \vec{w}'\| \leq 2\beta$

Binding if SIS is hard for $b = 2\beta$

Homomorphic Commitments from MSIS



- **Hiding:** (when adding some randomness)
- **Binding:** (based on SIS)
- **Homomorphic:**
- **(Succinct:)** (size $k \cdot \log q < \beta \cdot m$)

DLOG vs SIS

DLOG:

G group w/ generator g & order q

- $w \in \mathbb{Z}_q$ is witness
- $X = g^w$ is statement

- $g^w \cdot g^{w'} = g^{w+w'}$
- $(g^w)^c = g^{w \cdot c}$

- (Recall: Extends to $w \in \mathbb{Z}_q^m$)

SIS:

$A \in \mathbb{Z}_q^{k \times m}$ public matrix

- $\vec{w} \in \{-\beta, \dots, \beta\}^m$ is witness
- $X = A \cdot \vec{w}$ is statement

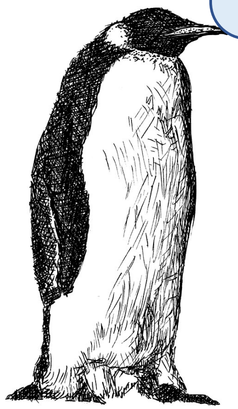
- $A \cdot \vec{w} + A \cdot \vec{w}' = A \cdot (\vec{w} + \vec{w}')$
- $c \cdot A \cdot \vec{w} = A \cdot (c \cdot \vec{w})$

@Khanh

Lattice-based Σ-Protocols

$\boxed{\vec{w}}$ =

I know value $\vec{w}$
such that $\boxed{\vec{w}}$
can be opened to $\vec{w}$



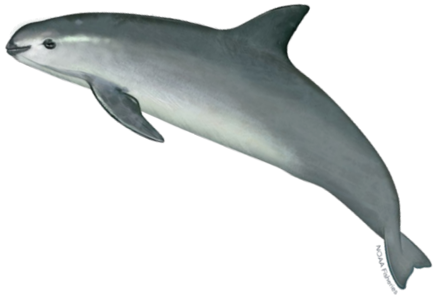
$\vec{r} \leftarrow \mathbb{Z}_q^m$

$\boxed{\vec{r}}$

$\boxed{\vec{w}}$

c

$c \leftarrow \mathbb{Z}_q$



$\vec{z} = \vec{r} + c \cdot \vec{w}$

Prover

Verifier (Vaquita)

- Complete: ✓
- HVZK: ✓
- Special Sound: ✗

Issue: Prover can choose $\vec{w}$ with arbitrary norm (easy task!) → Verifier will still accept!

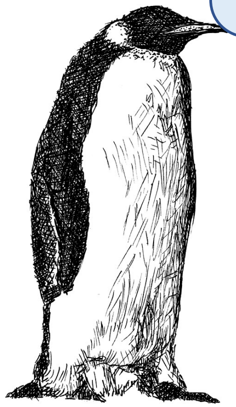
$$\boxed{\vec{z}} \stackrel{?}{=} \boxed{\vec{r}} + c \cdot \boxed{\vec{w}}$$

Lattice-based Σ-Protocols

$\boxed{\vec{w}}$ =

2. Attempt

I know value $\vec{w}$
such that $\boxed{\vec{w}}$
can be opened to $\vec{w}$

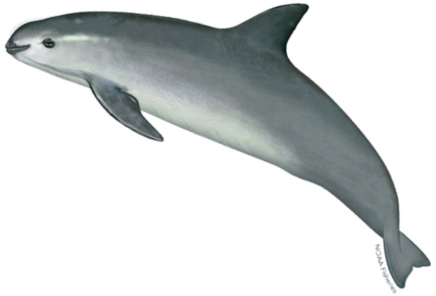


$\vec{r} \leftarrow \mathbb{Z}_q^m$

$\boxed{\vec{r}}$ $\longrightarrow$

$\longleftarrow$ c $\quad$ $c \leftarrow \mathbb{Z}_q$

$\vec{z} = \vec{r} + c \cdot \vec{w}$ $\longrightarrow$



Prover

Verifier (Vaquita)

- Complete: ❌

Issue: Even if $\vec{w}$ has small norm, the verifier will **not accept**!

$\boxed{\vec{z}} \stackrel{?}{=} \boxed{\vec{r}} + c \cdot \boxed{\vec{w}}$

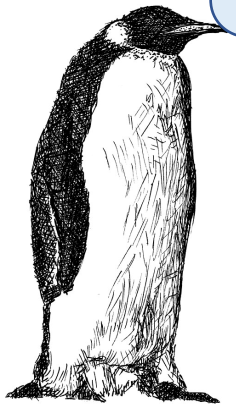
$\|\vec{z}\| \stackrel{?}{\leq} \beta$

Lattice-based Σ-Protocols

$\boxed{\vec{w}}$ =

3. Attempt

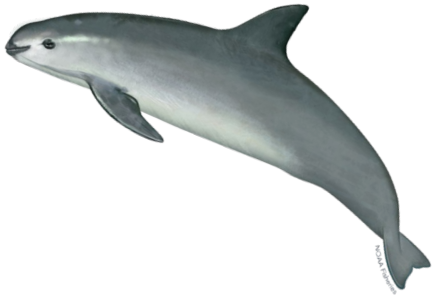
I know value $\vec{w}$ such that $\boxed{\vec{w}}$ can be opened to $\vec{w}$



$\vec{r} \leftarrow \{-\beta, \dots, \beta\}^m$ $\boxed{\vec{r}}$

c $\qquad c \leftarrow \mathbb{Z}_q$

$\vec{z} = \vec{r} + c \cdot \vec{w}$



$\boxed{\vec{w}}$

Prover

- Complete: ✗

Issue: Even if $\vec{w}$ has small norm, the verifier will **not accept**!

Verifier (Vaquita)

$$\boxed{\vec{z}} \stackrel{?}{=} \boxed{\vec{r}} + c \cdot \boxed{\vec{w}}$$

$$\|\vec{z}\| \stackrel{?}{\leq} \beta$$

Lattice-based Σ-Protocols

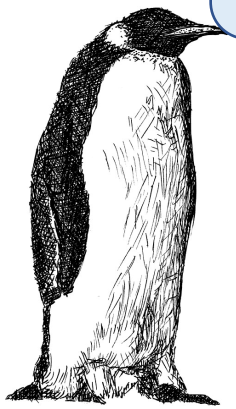
$\vec{w}$ =

4. Attempt

Issue:
- Want $||\vec{r}||$ large for **ZK**
- Want $||\vec{r}||$ small for **soundness**

$\vec{w}$

I know value $\vec{w}$ such that $\vec{w}$ can be opened to $\vec{w}$

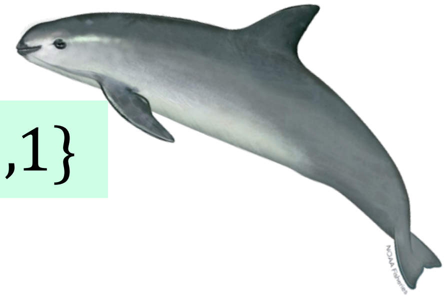


$\vec{r} \leftarrow \{-\beta, \dots, \beta\}^m$ $\quad \vec{r}$

c

$\vec{z} = \vec{r} + c \cdot \vec{w}$

$c \leftarrow \{0,1\}$



Prover

- Complete: ✓
- HVZK: ✗

Issue: Now $\vec{r}$ does not hide $\vec{w}$ anymore if $c = 1$ (e.g., $z_i = 2\beta \rightarrow w_i = \beta$)

Verifier (Vaquita)

$$\vec{z} \stackrel{?}{=} \vec{r} + c \cdot \vec{w}$$

$$||\vec{z}|| \stackrel{?}{\leq} 2\beta$$

Towards Soundness & ZK

Towards Soundness and ZK

Option 1: Choose very large parameters:

- $\vec{r} \leftarrow \{-B, \dots, B\}^m$ for $B \gg \beta$ (such that β/B is negligible)
- Choose large modulus q (such that SIS holds for large bound $b \in \mathcal{O}(B)$)
- **HVZK:** $\vec{z}$ only reveals something if $||\vec{z}|| > B - \beta$ (only happens with negl probability)
- **Soundness:** Given $\boxed{\vec{z}} \stackrel{?}{=} \boxed{\vec{r}} + 0 \cdot \boxed{\vec{w}}$ $\quad \boxed{\vec{z}'} \stackrel{?}{=} \boxed{\vec{r}} + 1 \cdot \boxed{\vec{w}'}$

$\vec{z}' - \vec{z}$ is valid opening for $\boxed{\vec{w}}$ with norm $\leq 2B$

Option 2:

- Choose smaller bound B
- Abort and restart if $\vec{z}$ would leak something [Lyubashevsky09,11]

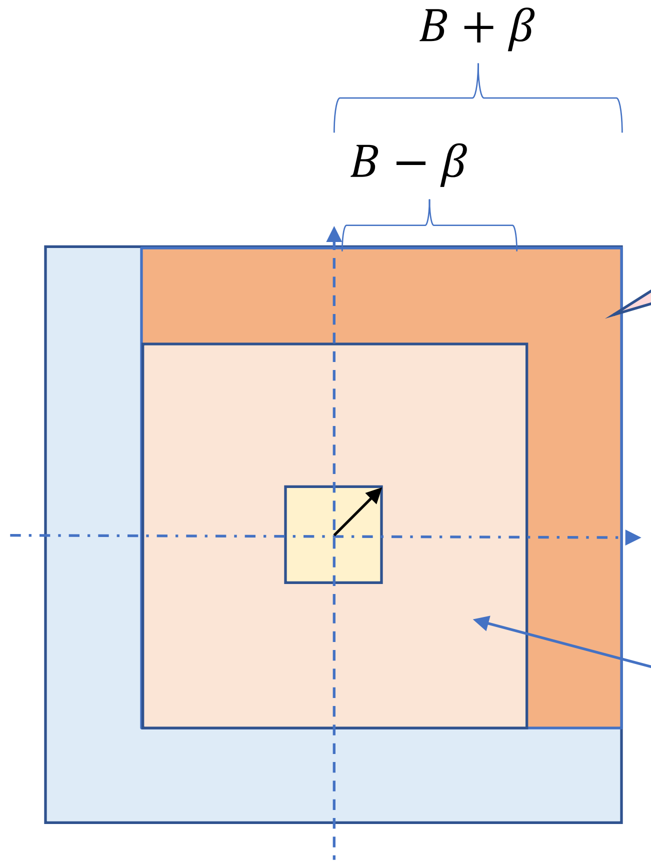
Soundness "Gap": Start with $||\vec{w}|| \leq \beta$ but can only extract $||\vec{w}'|| \leq 2B$

Rejection Sampling

Uniform distribution

Uniform Rejection Sampling

E.g., $\vec{w} = (\beta, \beta)$



Abort probability:

$$1 - \frac{(B-\beta)^m}{B^m}$$

Potential image of $\vec{z} = \vec{r} \ + c \cdot \vec{w}$ (for different $\vec{w}$)

Possible mage of $\vec{z} = \vec{r} \ + c \cdot \vec{w}$ for $\vec{w} = (\beta, \beta)$

Safe to reveal $\vec{z}$

$B \approx \beta$:

- Small parameters
- Abort probability ≈ 1

$B \gg \beta$:

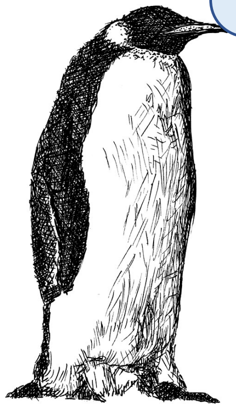
- Large parameters
- Abort probability ≈ 0

Lattice-based Σ-Protocols

$\boxed{\vec{w}}$ =

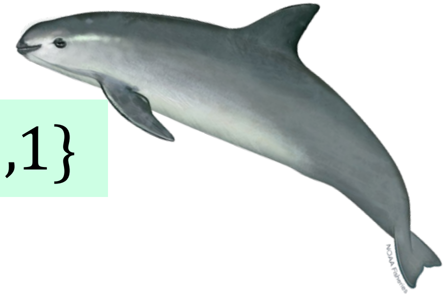
5. Attempt

I know value $\vec{w}$
such that $\boxed{\vec{w}}$
can be opened to $\vec{w}$



$\vec{r} \leftarrow \{-B, \dots, B\}^m$ $\boxed{\vec{r}}$ $\longrightarrow$

$\boxed{\vec{w}}$



c $\longleftarrow$ $c \leftarrow \{0,1\}$

If $\|z\| > B - \beta$
abort

$\vec{z} = \vec{r} + c \cdot \vec{w}$ $\longrightarrow$

Prover

Verifier (Vaquita)

- Complete: ✓
- HVZK (with abort): ✓
- Special Sound: ✓ (with soundness gap)

$$\boxed{\vec{z}} \overset{?}{=} \boxed{\vec{r}} + c \cdot \boxed{\vec{w}}$$

$$\|\vec{z}\| \overset{?}{\leq} B - \beta$$

Extending the Challenge Space

Extending the Challenge Space (1/3)

- **Problem:** Prover can cheat with probability ½
- What about challenge space $\mathcal{C} = \{-\delta, \ldots, \delta\}$ for small δ?
- **Example:** Extracting the witness for $c = -1$, $c' = 1$

$$\boxed{\vec{z}} \stackrel{?}{=} \boxed{\vec{r}} - 1 \cdot \boxed{\vec{w}} \qquad \boxed{\vec{z}'} \stackrel{?}{=} \boxed{\vec{r}} + 1 \cdot \boxed{\vec{w}'}$$

$2^{-1}(\vec{z}' - \vec{z})$ is valid opening for $\boxed{\vec{w}}$

Problem: 2^{-1} not small!

Can relax to ***approximate proofs***:
$\exists$ small $\gamma, \vec{w}$ st. $A \cdot \vec{w} = \gamma \cdot X$

Still limited challenge space

Note: *(important for the next talk)*

- Given approximate openings $A \cdot \vec{s_0} = \gamma_0 \cdot X$ and $A \cdot \vec{s_1} = \gamma_1 \cdot X$
- we get $A \cdot (\vec{s_0} \cdot \gamma_1 - \vec{s_1} \cdot \gamma_0) = \gamma_0 \cdot \gamma_1 \cdot X - \gamma_1 \cdot \gamma_0 \cdot X = 0$
- $\Rightarrow$ **Either** we get the *same fraction each time*, **or** *can solve SIS*

Extending the Challenge Space (2/3)

- **Polynomial ring** $R_q := \mathbb{Z}_q[X]/(f(X))$, e.g., $f(X) = X^d + 1$
- **Elements in** R_q: $a = a_0 + a_1 \cdot X + \cdots + a_{d-1} \cdot X^{d-1}$
- **Some facts:**
  - $X^d = -1$
  - $a + b = (\sum_{i=0}^{d-1} a_i \cdot X^i) + (\sum_{i=0}^{d-1} b_i \cdot X^i) = \sum_{i=0}^{d-1} (a_i + b_i) \cdot X^i$
  - $a \cdot b$
    $$= (\sum_{i=0}^{d-1} a_i \cdot X^i) \cdot (\sum_{i=0}^{d-1} b_i \cdot X^i) = \sum_{i=0}^{d-1} \left(\sum_{j,k: j+k=i} a_j \cdot b_k - \sum_{j,k: j+k=i+d} a_j \cdot b_k \right) \cdot X^i$$
  - $\|a + b\| \leq \|a\| + \|b\|$, $\|a \cdot b\| \leq d \cdot \|a\| \cdot \|b\|$

Extending the Challenge Space (3/3)

Here: consider infinity norm $||\vec{s}|| := \max_i ||s_i||$,
where $||s_i||$ denotes the larges coefficient of the polynomial s_i

- **MSIS Assumption:** It is difficult to find non-zero **module short integer solution** $\vec{s} \in R_q^m$ with $||\vec{s}|| \leq b$ and $A \cdot \vec{s} = 0 \bmod q$, where $A \in R_q^{k \times m}$

- Have more flexibility with the challenge space!
- (But: Challenge difference not necessarily invertible anymore)
- **For approximate proofs:** Can choose $\mathcal{C} := \{b_0 + b_1 X + \cdots + b_{d-1} X^{d-1} : b_0, \dots, b_{d-1} \in \{0,1\}\}$
- For $d \in \mathcal{O}(\lambda)$ we have exponential challenge space $|\mathcal{C}| = 2^d$

Approximate vs exact proofs

$$A \cdot \vec{w} = X$$

Approximate [Lyu09,Lyu11]:

- $\exists$ small $\gamma, \vec{w}$ st. $A \cdot \vec{w} = \gamma \cdot X$
- Sufficient for **signatures** like CRYSTALS-Dilithium
- Small proof sizes ($\approx 3KB$)

Exact:

- $\exists$ small $\vec{w}$ st. $A \cdot \vec{w} = X$
- Necessary for more advanced building blocks, e.g., verifiable encryption
- Much larger proof sizes

@Khanh

Thank you!