# Stern-Like Zero-Knowledge Protocol

Yanhong Xu

iCORE Information Security Laboratory
Department of Computer Science
University of Calgary, Canada

Feb 28, 2020

# Outline

1. Zero-Knowledge Proof System

2. Stern's Protocol

3. Decomposition and Extension

# Outline

# Physical Zero-Knowledge Proof System

Suppose I have a deck of card, and randomly pick one from it.

- Claim: I can tell whether it belongs to heart, spade, diamond, or club.
- Goal: I would like to convince you about my MAGIC ability.
- Solutions:

# Physical Zero-Knowledge Proof System

Suppose I have a deck of card, and randomly pick one from it.

- Claim: I can tell whether it belongs to heart, spade, diamond, or club.
- Goal: I would like to convince you about my MAGIC ability.
- Solutions:
  - Reveal the card to you.

# Physical Zero-Knowledge Proof System

Suppose I have a deck of card, and randomly pick one from it.

- Claim: I can tell whether it belongs to heart, spade, diamond, or club.
- Goal: I would like to convince you about my MAGIC ability.
- Solutions:
    - Reveal the card to you.
    - What if I do not want to show you which 1 out of 13 cards I have picked?

# Physical Zero-Knowledge Proof System

Suppose I have a deck of card, and randomly pick one from it.

- Claim: I can tell whether it belongs to heart, spade, diamond, or club.
- Goal: I would like to convince you about my MAGIC ability.
- Solutions:
  - Reveal the card to you.
  - What if I do not want to show you which 1 out of 13 cards I have picked?
  - Reveal the remaining 39 cards to you!

# Physical Zero-Knowledge Proof System (Cont.)

Is everyone convinced that I have the MAGIC ability?

- What if I am just lucky and guess it correct?

# Physical Zero-Knowledge Proof System (Cont.)

Is everyone convinced that I have the MAGIC ability?

- What if I am just lucky and guess it correct?
- Repeat as many times (say 100) as you want.

# Physical Zero-Knowledge Proof System (Cont.)

Is everyone convinced that I have the MAGIC ability?

- What if I am just lucky and guess it correct?
- Repeat as many times (say 100) as you want.
- The success probability of guessing them all correct is $\frac{1}{4^{100}} = 2^{-200}$.

# Physical Zero-Knowledge Proof System (Cont.)

Is everyone convinced that I have the MAGIC ability?

- What if I am just lucky and guess it correct?
- Repeat as many times (say 100) as you want.
- The success probability of guessing them all correct is $\frac{1}{4^{100}} = 2^{-200}$.

This is an actually interactive zero-knowledge proof.

- Completeness: if my claim is TRUE, then all of you will accept my claim.
- Soundness: if my claim is FALSE, then none of you accept my claim.
- Zero-Knowledge: No knowledge about which specific card I have picked.

Note that the protocol (without repetition) has soundness error $1/4$.
However, the protocol (with repetition 100) has soundness error $2^{-200}$.

# Preliminary

- NP relation $\rho \subseteq \{0,1\}^* \times \{0,1\}^*$: $(x, w) \in \rho$ is recognizable in polynomial time.
- NP language $\mathcal{L}_\rho$: $\{x : \exists\ w \text{ s.t. } |w| = \mathrm{poly}(|x|) \wedge (x, w) \in \rho\}$.
- $\mathrm{PPT}$ stands for probabilistic polynomial time.

# Interactive Zero-Knowledge Proof System

In 1985, Goldwasser, Micali and Rackoff [1] introduced the interactive zero-knowledge proof (ZKP).

Statment :$x \in \mathcal{L}_\rho$

$\mathcal{P}(x, w)$

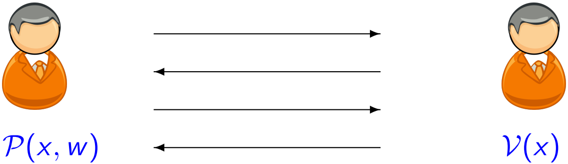
$\mathcal{V}(x)$

- $\mathcal{P}$ wants to convinces that $x \in \mathcal{L}_\rho$.

# Interactive Zero-Knowledge Proof System

In 1985, Goldwasser, Micali and Rackoff [1] introduced the interactive zero-knowledge proof (ZKP).

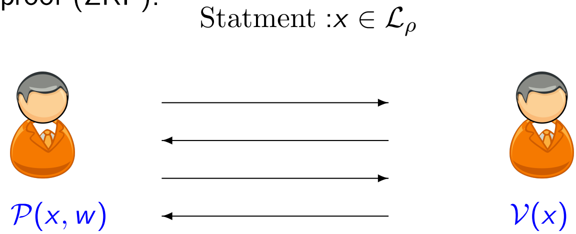
Statment : $x \in \mathcal{L}_\rho$




- $\mathcal{P}$ wants to convinces that $x \in \mathcal{L}_\rho$.

# Interactive Zero-Knowledge Proof System

In 1985, Goldwasser, Micali and Rackoff [1] introduced the interactive zero-knowledge proof (ZKP).

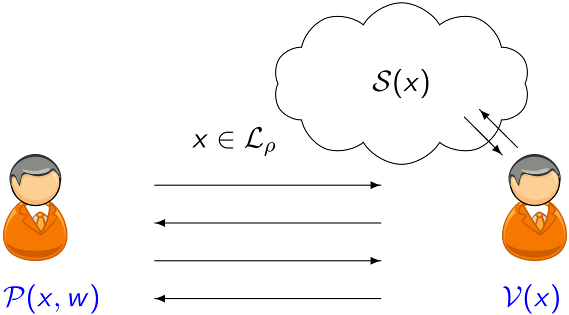



- $\mathcal{P}$ wants to convinces that $x \in \mathcal{L}_\rho$.
- $\mathcal{V}$ is convinced about the fact or reject.

# Interactive Zeor-Knowledge Proof System (Cont.)

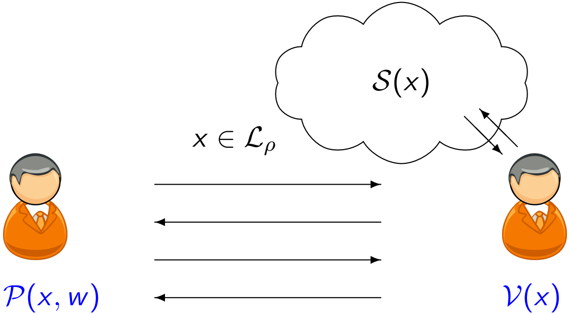
- $\mathcal{P}$ is $\mathrm{PPT}$, $\mathcal{V}$ is deterministic polynomial time.
- $\langle \mathcal{P}, \mathcal{V} \rangle$ form an interactive proof system for the language $\mathcal{L}_\rho$ if satisfies perfect completeness and soundness:
  - Completeness. For any $x \in \mathcal{L}_\rho$: $\Pr\big[\mathrm{Out}_{\mathcal{V}}\langle \mathcal{P}(x, w), \mathcal{V}(x)\rangle = 1\big] = 1$.
  - (Statistical) Soundness. For any $y \notin \mathcal{L}_\rho$ and for any $\widehat{\mathcal{P}}$:
    $\Pr[\mathrm{Out}_{\mathcal{V}}\langle \widehat{\mathcal{P}}(y), \mathcal{V}(y)\rangle = 1] \approx 0$.
    $\Rightarrow$ Proof system.
  - (Computational) Soundness. For any $y \notin \mathcal{L}_\rho$ and for any PPT $\widehat{\mathcal{P}}$:
    $\Pr[\mathrm{Out}_{\mathcal{V}}\langle \widehat{\mathcal{P}}(y), \mathcal{V}(y)\rangle = 1] \approx 0$.
    $\Rightarrow$ Argument system.
- Zero-Knowledge: nothing beyond the validity of the statement is revealed.

# Zero-Knowledge-Simulation Paradigm



# Zero-Knowledge-Simulation Paradigm

- Statistical zero-knowledge : for any $\mathcal{V}$, the simulated proof is indistinguishable from the real proof.
- Computational zero-knowledge: for any PPT $\mathcal{V}$ the simulated proof is indistinguishable from the real proof.



# Proof of Knowledge

Consider the following example.

- Let q be prime, and a group $\mathcal{G} =< g >$, where $g$ is the generator to the group.
- Suppose the Discrete Logarithm problem is hard for this group.
- Consider the language $\mathcal{L} = \{y : \exists x \in \mathbb{Z}_q \text{ s.t. } y = g^x\}$.
- Let $\langle \mathcal{P}, \mathcal{V} \rangle$ form an interactive proof system for $\mathcal{L}$.
- Trivial to show $y \in \mathcal{L}$; (why?)

# Proof of Knowledge

Consider the following example.

- Let q be prime, and a group $\mathcal{G} =< g >$, where $g$ is the generator to the group.
- Suppose the Discrete Logarithm problem is hard for this group.
- Consider the language $\mathcal{L} = \{y : \exists x \ \in \mathbb{Z}_q \text{ s.t. } y = g^x\}$.
- Let $\langle \mathcal{P}, \mathcal{V} \rangle$ form an interactive proof system for $\mathcal{L}$.
- Trivial to show $y \in \mathcal{L}$; (why?)
- More desirable to show possession/knowledge of $x$.
  $\rightarrow$ Proof of knowledge (Statistical soundness)
  $\rightarrow$ Argument of knowledge (Computational soundness)

# Outline

# Stern's Protocol-ZKAoK

- In 1996, Stern [4] introduced a three-move zero-knowledge argument of knowledge (ZKAoK) for the Syndrome Decoding (SD) problem in the coding theory.

**Definition (SD problem)**

Given uniformly random $\mathbf{A} \in \mathbb{Z}_2^{n\times m}$ and $\mathbf{y} \in \mathbb{Z}_2^n$. Let $w < m$ be an integer. The SD problem asks to find a vector $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

- $\rho_{\mathrm{stern}} = \{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_2^{n\times m} \times \mathbb{Z}_2^n \times \mathbb{Z}_2^m : (\mathrm{wt}(\mathbf{x}) = w) \wedge (\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2)\}$

# Stern's Protocol-ZKAoK

- In 1996, Stern [4] introduced a three-move zero-knowledge argument of knowledge (ZKAoK) for the Syndrome Decoding (SD) problem in the coding theory.

## Definition (SD problem)

Given uniformly random $\mathbf{A} \in \mathbb{Z}_2^{n \times m}$ and $\mathbf{y} \in \mathbb{Z}_2^n$. Let $w < m$ be an integer. The SD problem asks to find a vector $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

- $\rho_{\mathrm{stern}} = \{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_2^{n \times m} \times \mathbb{Z}_2^n \times \mathbb{Z}_2^m : (\mathrm{wt}(\mathbf{x}) = w) \wedge (\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2)\}$

## Stern's Idea

- For $\pi \in \mathcal{S}_m$, ($\mathbf{x} \in \{0,1\}^m$ satisfies $\mathrm{wt}(\mathbf{x}) = w$) $\Leftrightarrow$ ($\pi(\mathbf{x}) \in \{0,1\}^m$ also does)
- $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2 \Leftrightarrow \mathbf{A} \cdot (\mathbf{x} + \mathbf{r}) = \mathbf{y} + \mathbf{A} \cdot \mathbf{r} \bmod 2$.
- Commitment scheme COM: commit to a value and later reveal (decommit it).
  - Hiding and binding.

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

Prover | Verfier

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

| Prover | Verfier |
|---|---|
| 1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where $\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$ | |
| | 2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$. |

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

Prover

Verfier

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$.

3. If $ch = 1$, reveal $\mathbf{c}_2$ and $\mathbf{c}_3$. Send $\mathbf{v} = \pi(\mathbf{x})$ and $\mathbf{w} = \pi(\mathbf{r})$.

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

**Prover**

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

**Verfier**

2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$.

**Prover**

3. If $ch = 1$, reveal $\mathbf{c}_2$ and $\mathbf{c}_3$. Send $\mathbf{v} = \pi(\mathbf{x})$ and $\mathbf{w} = \pi(\mathbf{r})$.

**Verfier**

Check if $\mathbf{v} \in \mathbb{Z}_2^m$, $\mathrm{wt}(\mathbf{v}) = w$, and

$$\begin{cases} \mathbf{c}_2 = COM(\mathbf{w}); \\ \mathbf{c}_3 = COM(\mathbf{v} + \mathbf{w}). \end{cases}$$

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

| Prover | Verfier |
|---|---|
| 1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where $\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$ | |
| | 2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$. |
| 3. If $ch = 2$, reveal $\mathbf{c}_1$ and $\mathbf{c}_3$. Send $\pi$ and $\mathbf{z} = \mathbf{x} + \mathbf{r}$. | |

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

**Prover**

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

3. If $ch = 2$, reveal $\mathbf{c}_1$ and $\mathbf{c}_3$. Send $\pi$ and $\mathbf{z} = \mathbf{x} + \mathbf{r}$.

**Verfier**

2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$.

Check that

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{z} - \mathbf{y} \bmod 2); \\ \mathbf{c}_3 = COM(\pi(\mathbf{z})). \end{cases}$$

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

Prover

Verfier

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$.

3. If $ch = 3$, reveal $\mathbf{c}_1$ and $\mathbf{c}_2$. Send $\pi$ and $\mathbf{s} = \mathbf{r}$.

# Stern's Protocol (cont.)

- Common input: $\mathbf{A}, \mathbf{y}$.
- Prover's goal: Convince the verifier in ZK that he knows $\mathbf{x} \in \mathbb{Z}_2^m$ such that $\mathrm{wt}(\mathbf{x}) = w$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod 2$.

**Prover**

1. Pick $\mathbf{r} \xleftarrow{\$} \mathbb{Z}_2^m$, $\pi \xleftarrow{\$} \mathcal{S}_m$. Send $(\mathbf{c}_1, \mathbf{c}_2, \mathbf{c}_3)$, where

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{r} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{r})); \\ \mathbf{c}_3 = COM(\pi(\mathbf{x} + \mathbf{r})). \end{cases}$$

3. If $ch = 3$, reveal $\mathbf{c}_1$ and $\mathbf{c}_2$. Send $\pi$ and $\mathbf{s} = \mathbf{r}$.

**Verfier**

2. Send a challenge $ch \xleftarrow{\$} \{1, 2, 3\}$.

Check that

$$\begin{cases} \mathbf{c}_1 = COM(\pi, \mathbf{A} \cdot \mathbf{s} \bmod 2); \\ \mathbf{c}_2 = COM(\pi(\mathbf{s})). \end{cases}$$

# Analysis of Stern's Protocol

- Completeness.
- Soundness: soundness error $2/3$.
- Statistical zero-knowledge: the commitment scheme COM, the masking vector $\mathbf{r}$, and the permutation $\pi$.
- Argument of knowledge.

Repeat the protocol enough times to achieve negligible soundness error.

# Development

- In 2008, Kawachi et al. [2] adapted Stern's protocol to the lattice setting by working with $q$.
  - $\rho_{\mathrm{ktx}} = \{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_q^{n\times m} \times \mathbb{Z}_q^n \times \{0,1\}^m : (\mathrm{wt}(\mathbf{x}) = w) \wedge (\mathbf{A}\cdot\mathbf{x} = \mathbf{y} \bmod q)\}$
  - A restricted version of the Inhomogeneous Short Integer Solution(ISIS) problem.

**Definition (ISIS$_{n,m,q,\beta}$)**

Given uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n\times m}$ and $\mathbf{y} \in \mathbb{Z}_q^n$. Let $\beta$ be a real number. The ISIS problem asks to find a vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\|\mathbf{x}\|_\infty \leq \beta$ and $\mathbf{A}\cdot\mathbf{x} = \mathbf{y} \bmod q$.

- Limited applications.

# Development

- In 2008, Kawachi et al. [2] adapted Stern's protocol to the lattice setting by working with $q$.
  - $\rho_{\text{ktx}} = \{((\mathbf{A}, \mathbf{y}), \mathbf{x}) \in \mathbb{Z}_q^{n \times m} \times \mathbb{Z}_q^n \times \{0,1\}^m : (\mathrm{wt}(\mathbf{x}) = w) \wedge (\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q)\}$
  - A restricted version of the Inhomogeneous Short Integer Solution(ISIS) problem.

**Definition (ISIS$_{n,m,q,\beta}$)**

Given uniformly random $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ and $\mathbf{y} \in \mathbb{Z}_q^n$. Let $\beta$ be a real number. The ISIS problem asks to find a vector $\mathbf{x} \in \mathbb{Z}_q^m$ such that $\|\mathbf{x}\|_\infty \leq \beta$ and $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$.

  - Limited applications.

- In 2013, Ling et al. [3] removed the restrictions on $\mathbf{x}$ and proposed a Stern-like zero-knowledge protocol for the ISIS problem.
  - Decomposition and extension.
  - Wide applications: policy-based signatures, group encryption, **group signatures**, and much more.

# Outline

# Decomposition and Extension

ZKAoK for Restricted SIS [2]

$(\mathbf{x} \in \{0,1\}^m) \wedge (\mathrm{wt}(\mathbf{x}) = w)$

↑ Extension

$\mathbf{x} \in \{0,1\}^m$

↑ Decomposition

$\|\mathbf{x}\|_\infty \leq \beta$

ZKAoK for General SIS

# Extension

Goal: $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ and $\mathbf{x} \in \{0,1\}^m$.

Intermediate goal: $\mathbf{A}^* \cdot \mathbf{x}^* = \mathbf{y} \bmod q$ and $\mathbf{x}^* \in \{0,1\}^m$ and $\mathbf{x}^*$ has fixed hamming weight.

- Let $\mathsf{B}_{3m}$ be the set of all vectors in $\{0,1\}^{3m}$ such that each vector contains exactly $m$ copies of 0, $m$ copies of 1.
- Extend $\mathbf{x} \in \{0,1\}^m$ to $\mathbf{x}^* \in \mathsf{B}_{2m}$.
- Observe that $\mathrm{wt}(\mathbf{x}^*) = m$.

# Extension

Goal: $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ and $\mathbf{x} \in \{0,1\}^m$.

Intermediate goal: $\mathbf{A}^* \cdot \mathbf{x}^* = \mathbf{y} \bmod q$ and $\mathbf{x}^* \in \{0,1\}^m$ and $\mathbf{x}^*$ has fixed hamming weight.

- Let $\mathsf{B}_{3m}$ be the set of all vectors in $\{0,1\}^{3m}$ such that each vector contains exactly $m$ copies of 0, $m$ copies of 1.
- Extend $\mathbf{x} \in \{0,1\}^m$ to $\mathbf{x}^* \in \mathsf{B}_{2m}$.
- Observe that $\mathrm{wt}(\mathbf{x}^*) = m$.
- Extend $\mathbf{A} \in \mathbb{Z}_q^{n \times m}$ to $\mathbf{A}^* \in \mathbb{Z}_q^{n \times m}$ such that $\mathbf{A} \cdot \mathbf{x} = \mathbf{A}^* \cdot \mathbf{x}^* \bmod q$. (how and why?)

A ZKAoK protocol for the ISIS problem with $\|\mathbf{x}\|_\infty = 1$.

# Decomposition

Let $\beta \in \mathbb{Z}^+$.
Goal: $\mathbf{A} \cdot \mathbf{x} = \mathbf{y} \bmod q$ and $\mathbf{x} \in [0, \beta]^m$.

Intermediate goal: $\mathbf{A}^* \cdot \mathbf{x}^* = \mathbf{y} \bmod q$ and $\mathbf{x}^*$ is binary.

Define $\delta_\beta = \lfloor \log \beta \rfloor + 1$. Define the sequence $\beta_1, \ldots, \beta_{\delta_\beta}$ as follows.

$\beta_1 = \lceil \beta/2 \rceil$, $\beta_2 = \lceil (\beta - \beta_1)/2 \rceil$, $\beta_3 = \lceil (\beta - \beta_1 - \beta_2)/2 \rceil, \ldots, \beta_{\delta_\beta} = 1$.

**Example.** Let $\beta = 50$, then $\delta_\beta = 6$,

$$\beta_1 = 25, \beta_2 = 13, \beta_3 = 6, \beta_4 = 3, \beta_5 = 2, \beta_6 = 1.$$

Notice that $\sum_{i=1}^{6} \beta_i = \beta$.

# Decomposition (cont.)

- Properties: $\sum_{i=1}^{\delta} \beta_i = \beta$. For any $b \in [0, \beta]$, there exists $b^{(1)}, \ldots, b^{(\delta_\beta)} \in \{0,1\}$ such that $\sum_{i=1}^{\delta_\beta} \beta_i \cdot b^{(i)} = b$. Define $\mathrm{idec}(b) = (b^{(1)}, \ldots, b^{(\delta_\beta)})^\top \in \{0,1\}^{\delta_\beta}$.
- For $m \in \mathbb{Z}^+$, define a matrix $\mathbf{G}_{m,\beta} \in \mathbb{Z}^{m \times m\delta_\beta}$ to be

$$\mathbf{G}_{m,\beta} = \begin{bmatrix} \beta_1 \ldots \beta_{\delta_\beta} & & \\ & \ddots & \\ & & \beta_1 \ldots \beta_{\delta_\beta} \end{bmatrix}$$

- For $\mathbf{x} = (x_1, \ldots, x_m)^\top \in [0, \beta]$, define $\mathrm{vdec}(\mathbf{x}) = (\mathrm{idec}(x)_1 \| \ldots \| \mathrm{idec}(x)_m) \in \{0,1\}^{m\delta_\beta}$.
- We then have $\mathbf{x} = \mathbf{G}_{m,\beta} \cdot \mathrm{vdec}(\mathbf{x}) \bmod q$.
- Observe that $\mathbf{A} \cdot \mathbf{x} = \mathbf{A} \cdot \mathbf{G}_{m,\beta} \cdot \mathrm{vdec}(\mathbf{x}) \bmod q \triangleq \mathbf{A}^* \cdot \mathrm{vdec}(\mathbf{x}) \bmod q$.

A ZKAoK protocol for the ISIS problem with $\|\mathbf{x}\|_\infty \leq \beta$.

# Thank You

Thank you!

Any Questions?

S. Goldwasser, S. Micali, and C. Rackoff.
The knowledge complexity of interactive proof-systems (extended abstract).
In *ACM STOC 1985*, pages 291–304. ACM, 1985.

A. Kawachi, K. Tanaka, and K. Xagawa.
Concurrently secure identification schemes based on the worst-case hardness of lattice problems.
In *ASIACRYPT 2008*, volume 5350 of *LNCS*, pages 372–389. Springer, 2008.

S. Ling, K. Nguyen, D. Stehlé, and H. Wang.
Improved zero-knowledge proofs of knowledge for the ISIS problem, and applications.
In *PKC 2013*, volume 7778 of *LNCS*, pages 107–124. Springer, 2013.

J. Stern.
A new paradigm for public key identification.
*IEEE Trans. Information Theory*, 42(6):1757–1768, 1996.