

# Set-Membership Proof

---

Using Bulletproofs

# Set Membership

- Goal: Prove that a **secret value  $v$**  is in a **public set  $S$** .
  - For example:  $v = \text{"DK"}$  and  $S = \{\text{"DE"}, \text{"DK"}, \text{"UK"}, \text{"FR"}, \text{"UK"}\}$
  - The efficiency of the proof will depend on  $|S|$ .

Fancy Proof: E.g. Curve Trees

Complex  
Implementation

Medium to Large  $S$

Small  $S$

Medium  $S$

Sigma OR

Our BP adaption

$(v=1)$  or  $(v=3)$  or  $(v=5)$

**Finite field**, + and \* are mod  $q$

$$\mathbb{F}_q = \{0, \dots, q - 1\}$$

Very large **prime number**

# Numbers

Everything is a number,

- “DK” -> 0x444b

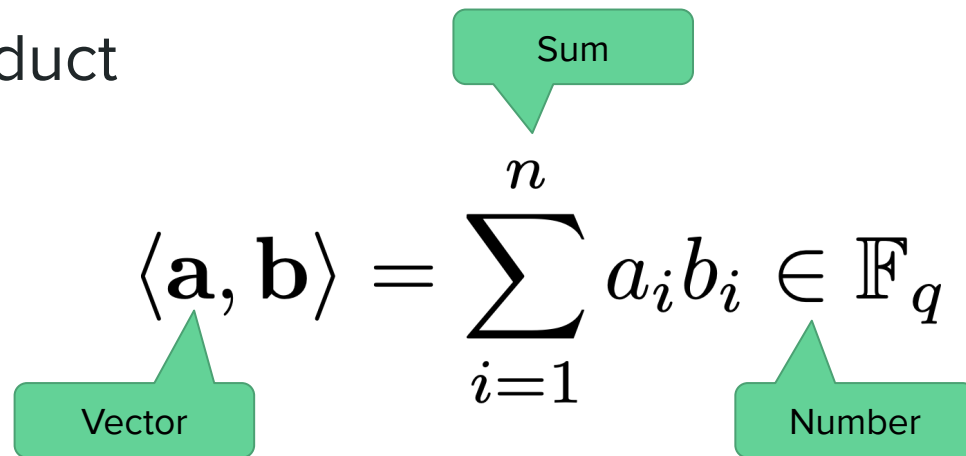
$$\mathbf{a} = \begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \in \mathbb{F}_q^n$$

A list of n number in  $0..q-1$

# Vectors

Ordered lists of numbers

# Inner Product



The diagram shows the inner product formula  $\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n a_i b_i \in \mathbb{F}_q$ . Annotations include a green box labeled "Sum" pointing to the summation symbol, a green box labeled "Vector" pointing to  $\mathbf{a}$ , and a green box labeled "Number" pointing to  $b_i$ .

$$\langle \mathbf{a}, \mathbf{b} \rangle = \sum_{i=1}^n a_i b_i \in \mathbb{F}_q$$

$$\left\langle \begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix}, \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} \right\rangle = 1 \cdot 4 + 2 \cdot 5 + 3 \cdot 6 = 32$$

q is very large

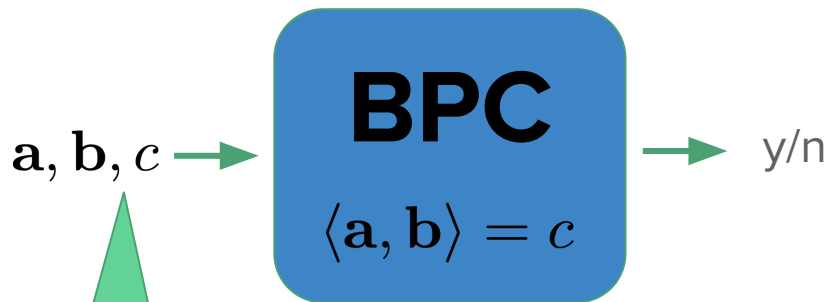
# Hadamard Product

$$\mathbf{a} \circ \mathbf{b} = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_n b_n \end{pmatrix} \in \mathbb{F}_q^n$$

Diagram illustrating the Hadamard Product operation. Two vectors,  $\mathbf{a}$  and  $\mathbf{b}$ , are multiplied element-wise to produce a new vector. The result is shown as a column vector with elements  $a_1 b_1, \dots, a_n b_n$ , which belongs to the field  $\mathbb{F}_q^n$ . Green callouts identify the input vectors and the result vector.

$$\begin{pmatrix} 1 \\ 2 \\ 3 \end{pmatrix} \circ \begin{pmatrix} 4 \\ 5 \\ 6 \end{pmatrix} = \begin{pmatrix} 4 \\ 10 \\ 18 \end{pmatrix}$$

q is very large



Vectors and value  
may be secret

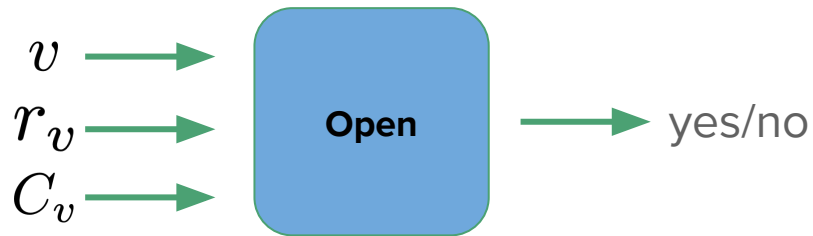
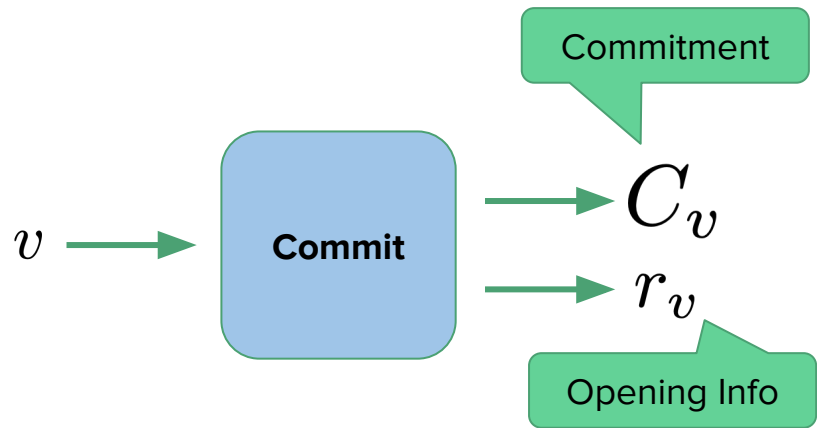
# Bulletproofs

At the core an inner product  
proof

# Interlude: Commit-and-Proof

---



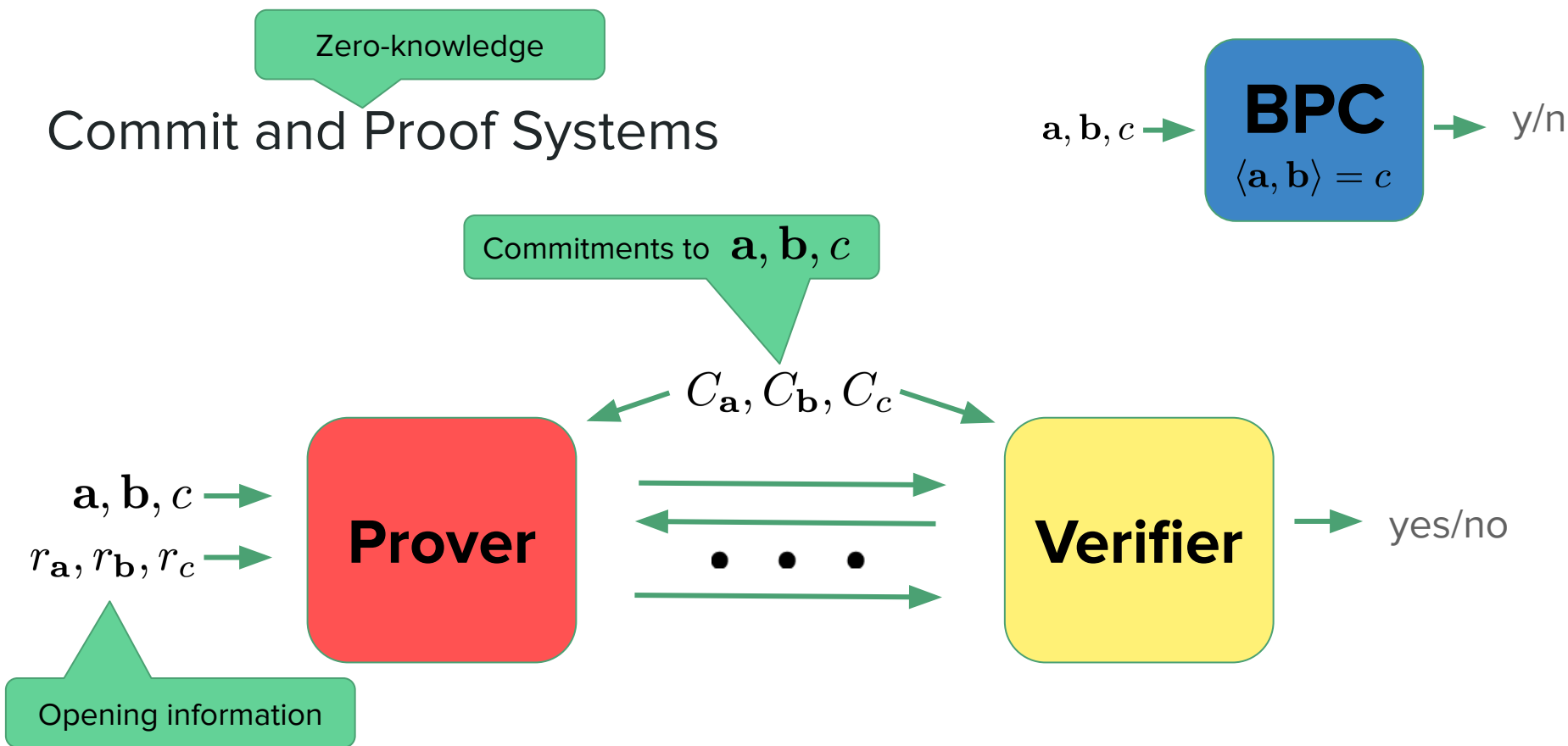


*Commitment  $\sim$  Envelope with value inside*

# Commitments

Something with Pedersen

# Commit and Proof Systems

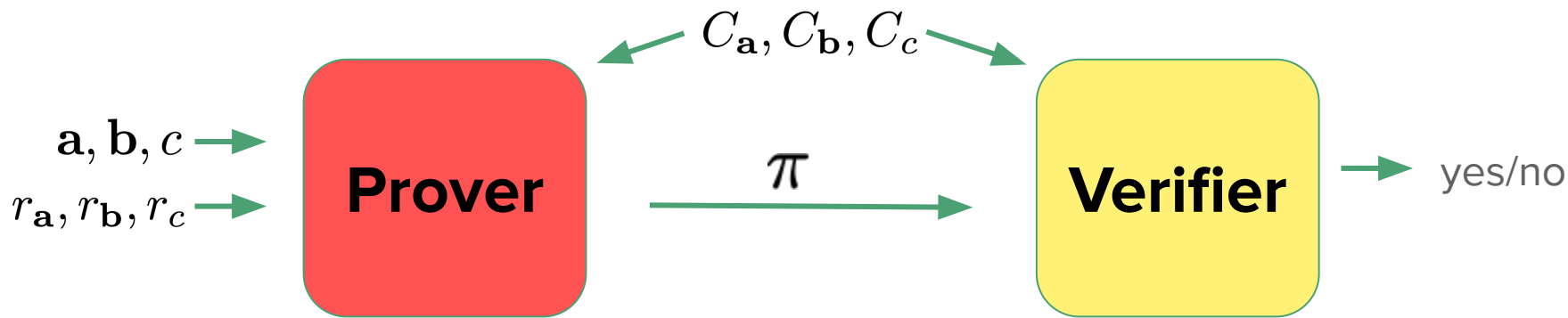
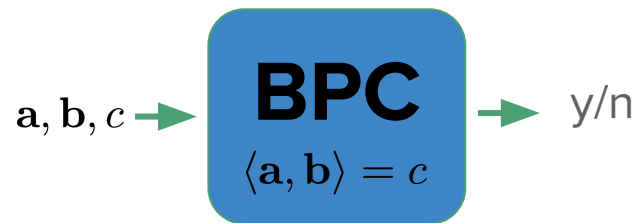


*"I can open the given commitments to values such that they satisfy the inner product relation."*

# Commit and Proof Systems

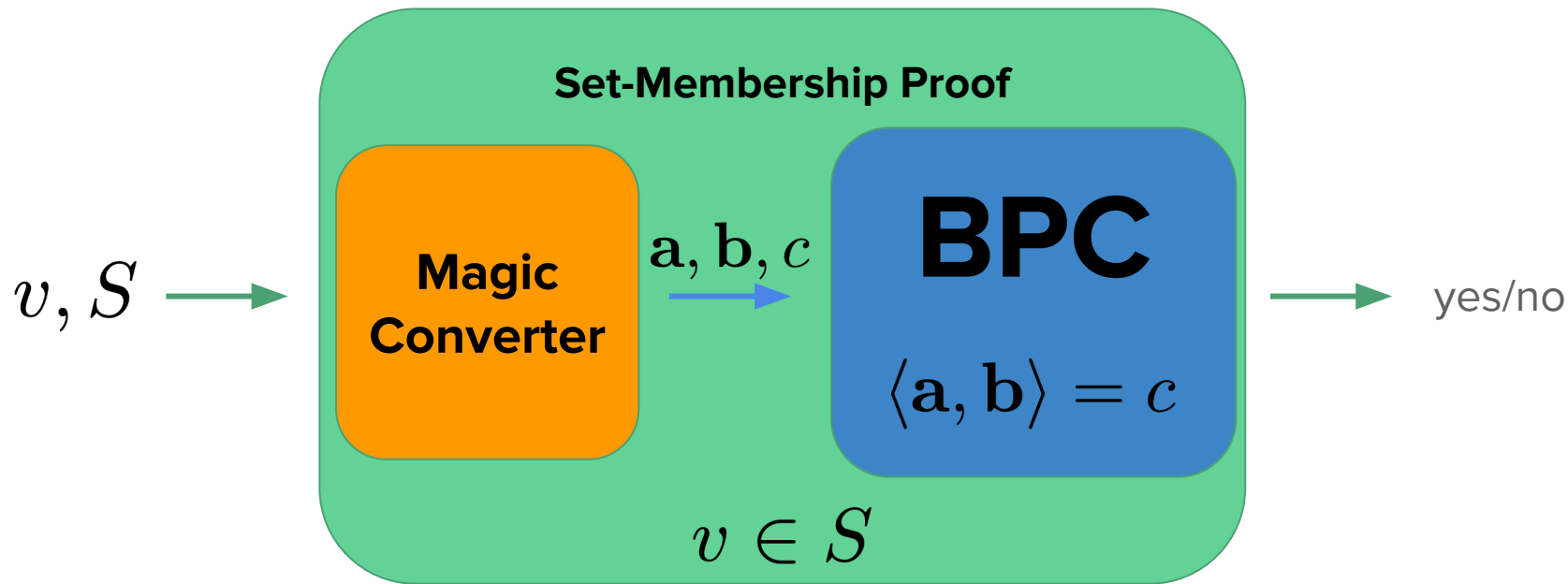
Zero-knowledge

Non-Interactive



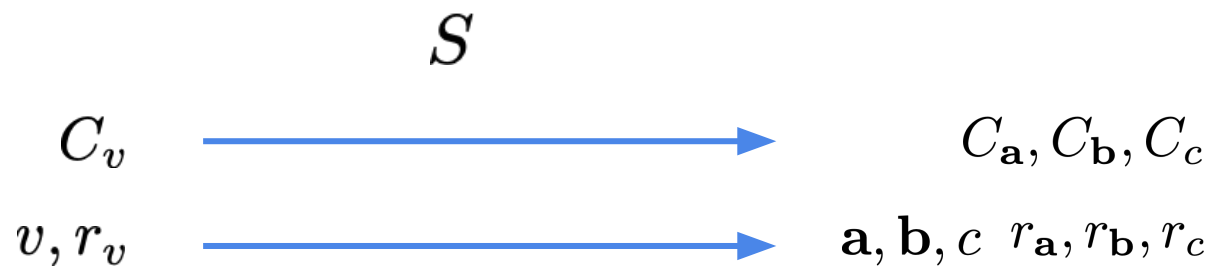
*"I can open the given commitments to values such that they satisfy the inner product relation."*

## Set-membership - Construction Idea



$$v \in S \Leftrightarrow \langle \mathbf{a}, \mathbf{b} \rangle = c$$

# Set-membership - Converter



Number

$$P(X) = a_n X^n + \cdots + a_1 X + a_0$$

Finding ~~None~~ Roots

$$P(X) = 0$$

Unless P is zero-polynomial

There are at most n roots.

Example

$$X^2 - 4$$

Coefficients  
Vector

$$\begin{pmatrix} 1 \\ 0 \\ -4 \end{pmatrix}$$

2 is a root

A very large number (mod q)

# Polynomials

This is where X comes into play

# Schwartz-Zippel Lemma

$$P(X) = a_n X^n + \cdots + a_1 X + a_0 \in \mathbb{F}_q[X]$$

$y \xleftarrow{\$} \mathbb{F}_q$  random number

P not zero-polynomial

small

$$\Pr[P(y) = 0] \leq \frac{n}{|\mathbb{F}_q|} = \frac{n}{q}$$

very unlikely

very large

P zero polynomial

$$\Pr[P(y) = 0] = 1$$

# Main Trick

Check if

$$\begin{pmatrix} a_1 \\ \vdots \\ a_n \end{pmatrix} \stackrel{?}{=} \begin{pmatrix} 0 \\ \vdots \\ 0 \end{pmatrix}$$

coefficients vector

zero polynomial

$$y \xleftarrow{\$} \mathbb{F}_q$$

**S.Z.**

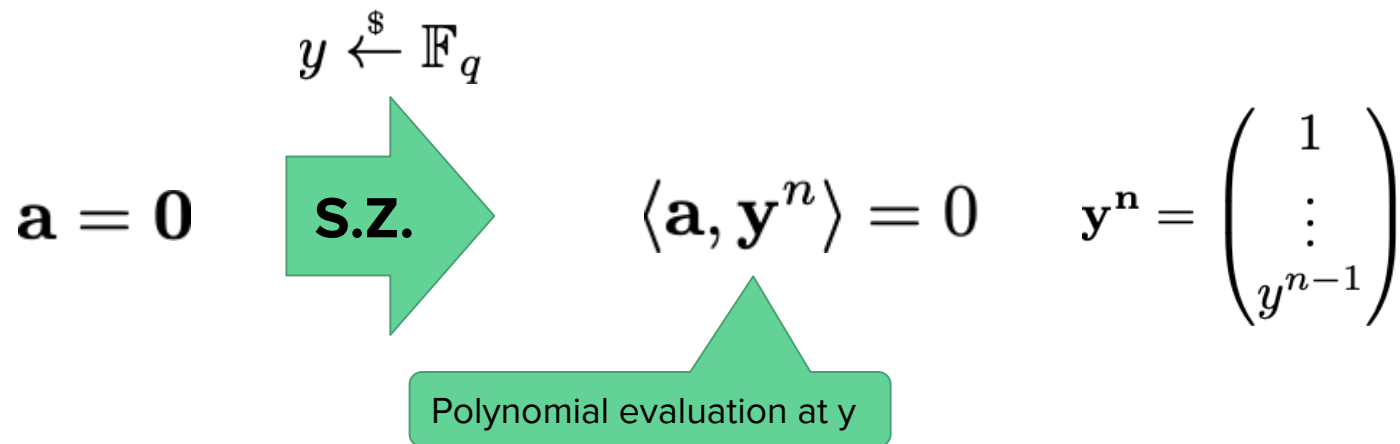
$$\sum_{i=1}^n a_i y^{i-1} \stackrel{?}{=} 0 = \sum_{i=1}^n 0 y^{i-1}$$

Equivalent to  
original equation  
w.h.p.

Polynomial evaluation at y



# Main Trick



# Set-membership Proof

---

# Set-Membership - Reduction to Inner Product

$$v \in S = \{s_1, \dots, s_n\} \quad v = s_i$$

*"I know  $v$  is in  $S$ "*

Vectorize

at position  $i$

$$\mathbf{s} = (s_1, \dots, s_n)^\top \quad \mathbf{a}_L = (0, \dots, 1, \dots, 0)^\top$$

$$\langle \mathbf{s}, \mathbf{a}_L \rangle = v$$

*"I know the index  $i$  such that  $v = s_i$ "*

## Set-Membership - Reduction to Inner Product $v \in \mathcal{S}$

$$\mathbf{s} = (s_1, \dots, s_n)^\top \quad \mathbf{a}_L = (0, \dots, 1, \dots, 0)^\top \quad \langle \mathbf{s}, \mathbf{a}_L \rangle = v$$

public

secret  $\rightarrow$  untrusted

at position  $i$

Consistency checks for  $\mathbf{a}_L$  // zero vector with exactly one 1

$$\mathbf{a}_R := \mathbf{a}_L - \mathbf{1}$$

$$\langle \mathbf{a}_L, \mathbf{1} \rangle = 1 \quad // \text{coefficients sum up to 1}$$

$$\mathbf{a}_L \circ \mathbf{a}_R = \mathbf{0} \quad // \text{for each coordinates one of them is zero}$$

$$(\mathbf{a}_L - \mathbf{1}) - \mathbf{a}_R = \mathbf{0} \quad // \mathbf{a}_R \text{ is really } \mathbf{a}_L - \mathbf{1}$$

# Set-Membership - Reduction to Inner Product $v \in \mathcal{S}$

$$\mathbf{s} = (s_1, \dots, s_n)^\top \quad \mathbf{a}_L = (0, \dots, 1, \dots, 0)^\top \quad \mathbf{a}_R := \mathbf{a}_L - \mathbf{1}$$

Equations:

$$\langle \mathbf{s}, \mathbf{a}_L \rangle = v$$

$$\langle \mathbf{a}_L, \mathbf{1} \rangle = 1$$

$$\mathbf{a}_L \circ \mathbf{a}_R = \mathbf{0}$$

$$(\mathbf{a}_L - \mathbf{1}) - \mathbf{a}_R = \mathbf{0}$$

$$y \xleftarrow{\$} \mathbb{F}_q$$



$$\langle \mathbf{a}_L, \mathbf{s} \rangle = v,$$


$$\langle \mathbf{a}_L, \mathbf{1} \rangle = 1,$$

$$\langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle = 0,$$

$$\langle \mathbf{a}_L - \mathbf{1} - \mathbf{a}_R, \mathbf{y}^n \rangle = 0.$$

Set-Membership - Reduction to Inner Product  $v \in \mathcal{S}$

$$\mathbf{s} = (s_1, \dots, s_n)^\top \quad \mathbf{a}_L = (0, \dots, 1, \dots, 0)^\top \quad \mathbf{a}_R := \mathbf{a}_L - \mathbf{1}$$

$$\begin{aligned} \langle \mathbf{a}_L, \mathbf{s} \rangle &= v, & z &\stackrel{\$}{\leftarrow} \mathbb{F}_q \\ \langle \mathbf{a}_L, \mathbf{1} \rangle &= 1, \\ \langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle &= 0, \\ \langle \mathbf{a}_L - \mathbf{1} - \mathbf{a}_R, \mathbf{y}^n \rangle &= 0. \end{aligned}$$

$$z^3 + z^2v = z^3 \langle \mathbf{a}_L, \mathbf{1} \rangle + z^2 \langle \mathbf{a}_L, \mathbf{s} \rangle + z \langle \mathbf{a}_L - \mathbf{1} - \mathbf{a}_R, \mathbf{y}^n \rangle + \langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle$$

## Set-Membership - Reduction to Inner Product $v \in S$

$$\mathbf{s} = (s_1, \dots, s_n)^\top \quad \mathbf{a}_L = (0, \dots, 1, \dots, 0)^\top \quad \mathbf{a}_R := \mathbf{a}_L - \mathbf{1}$$

$$z^3 + z^2v = z^3\langle \mathbf{a}_L, \mathbf{1} \rangle + z^2\langle \mathbf{a}_L, \mathbf{s} \rangle + z\langle \mathbf{a}_L - \mathbf{1} - \mathbf{a}_R, \mathbf{y}^n \rangle + \langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle$$

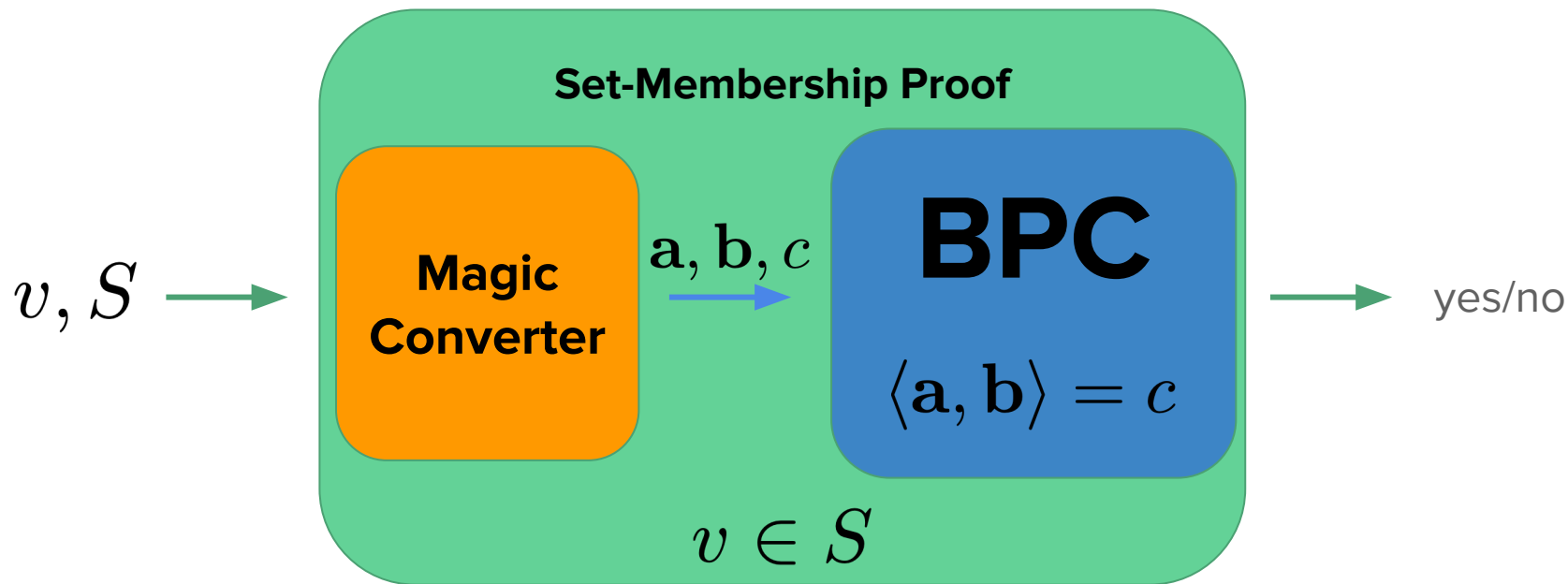
public function



Rewriting the  
equation in a clever  
way

$$z^2v + \delta(y, z) = \langle \mathbf{a}_L - z\mathbf{1}, \mathbf{y}^n \circ (\mathbf{a}_R + z\mathbf{1}) + z^3\mathbf{1} + z^2\mathbf{s} \rangle$$

## Set-membership - Construction Idea



$$v \in S \Leftrightarrow \langle \mathbf{a}, \mathbf{b} \rangle = c$$



# Set-Non-Membership

$$v \notin S = \{s_1, \dots, s_n\} \quad \text{"I know } v \text{ is not in } S\text{"}$$



$$\forall i \quad v \neq s_i \quad \text{"I know } v \text{ is not } s_i \text{ for any } i\text{"}$$



$$\forall i \quad v - s_i \neq 0 \quad \text{"I know the difference of } v \text{ and } s_i \text{ is not zero for any } i\text{"}$$



Finite field

$$\forall i \exists a_i \quad a_i(v - s_i) = 1 \quad \text{"I know the multiplicative inverse of } (v-s_i) \text{ for any } i\text{"}$$

## Set-Non-Membership

$v \notin S = \{s_1, \dots, s_n\}$  “I know  $v$  is not in  $S$ ”

$\Leftrightarrow$

$\mathbf{a}_L = (a_0, \dots, a_{n-1})$  and  $\mathbf{a}_R = v\mathbf{1}$

$$\mathbf{a}_L \circ (\mathbf{a}_R - \mathbf{s}) = \mathbf{1},$$

$$\mathbf{a}_R = v\mathbf{1}.$$