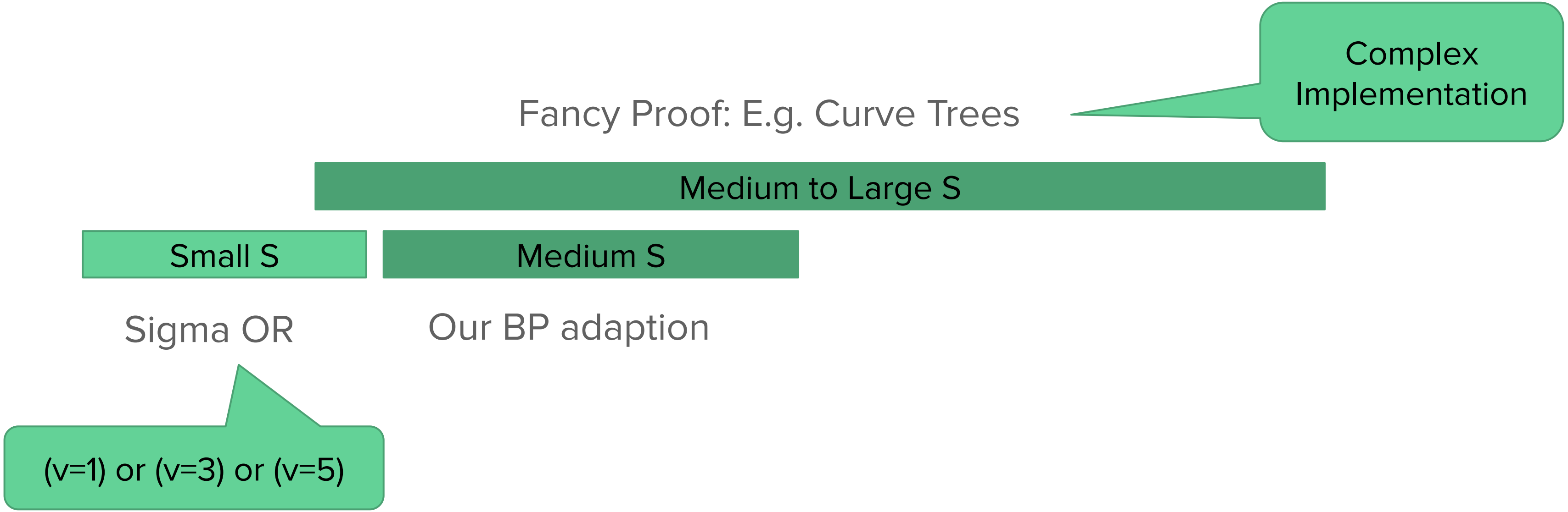
Set-Membership Proof

Using Bulletproofs

Slides with permission from Daniel

Set Membership

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



Finite field, + and * are mod q

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

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

Sum

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

Vector

Number

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

q is very large

Hadamard Product

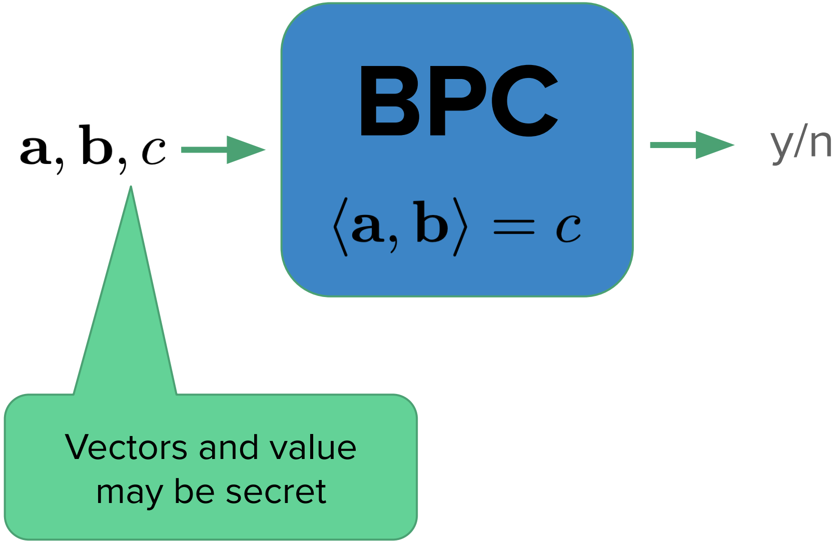
$$\mathbf{a} \circ \mathbf{b} = \begin{pmatrix} a_1 b_1 \\ \vdots \\ a_n b_n \end{pmatrix} \in \mathbb{F}_q^n$$

Vector

Vector

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

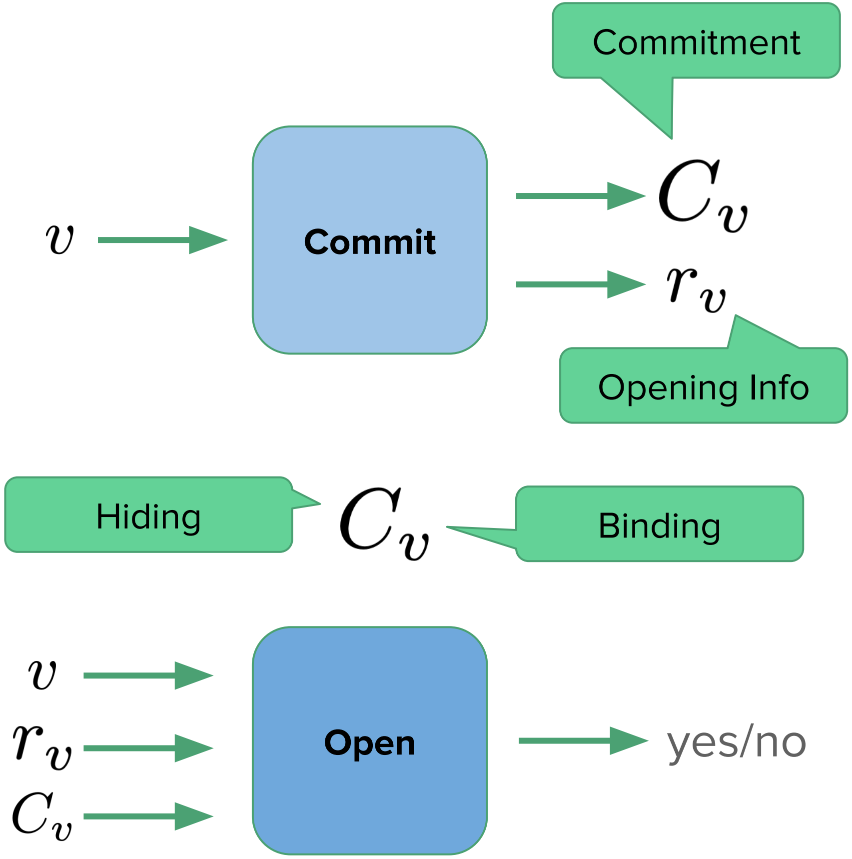
q is very large



Bulletproofs

At the core an inner product proof

Interlude: Commit-and-Proof

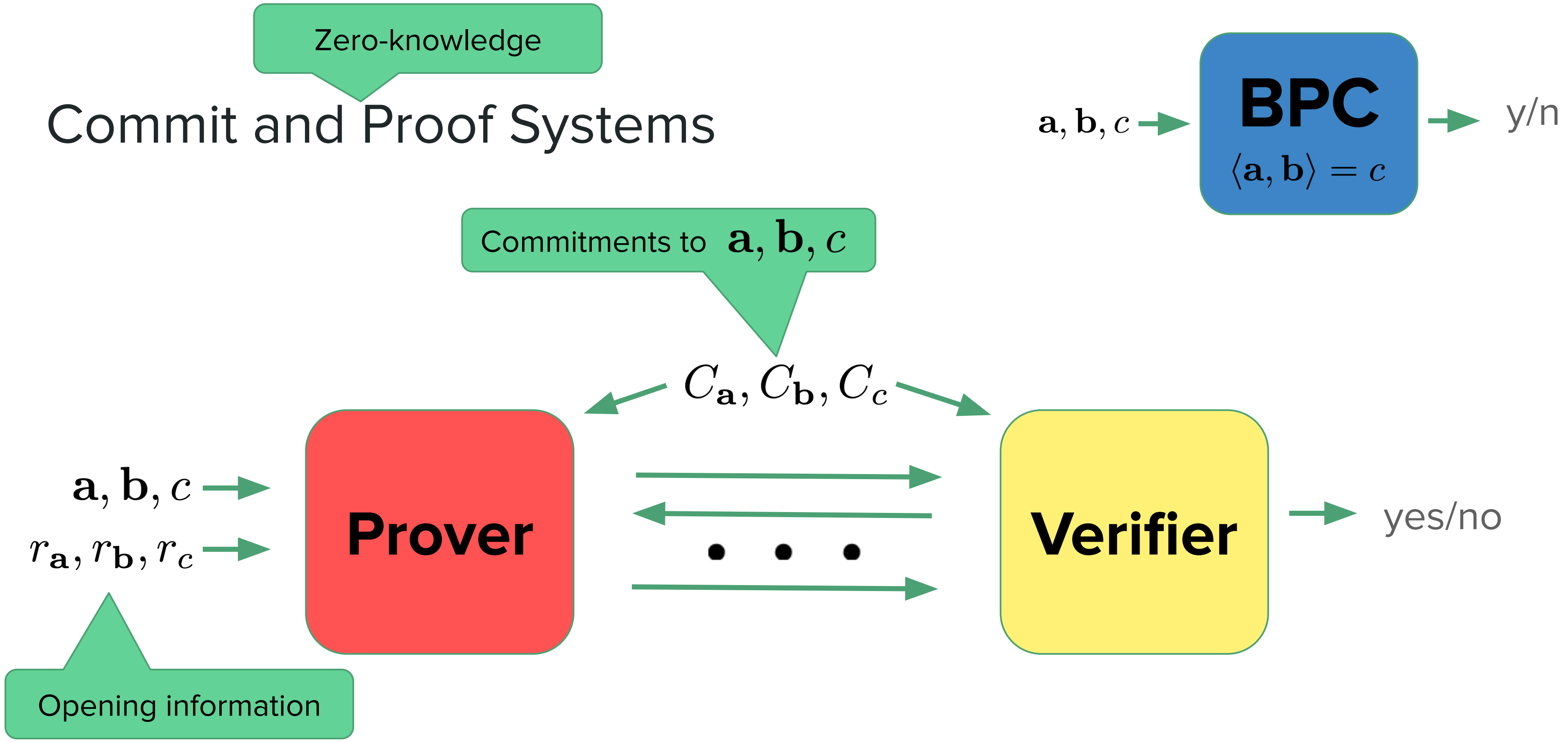


Commitment ~ Envelope with value inside

Commitments

Something with Pedersen

Commit and Proof Systems

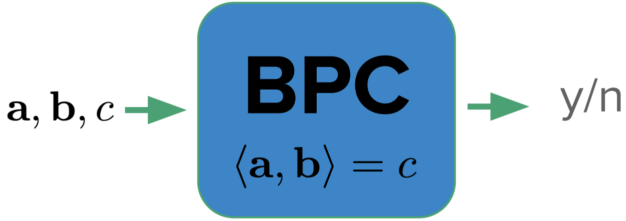


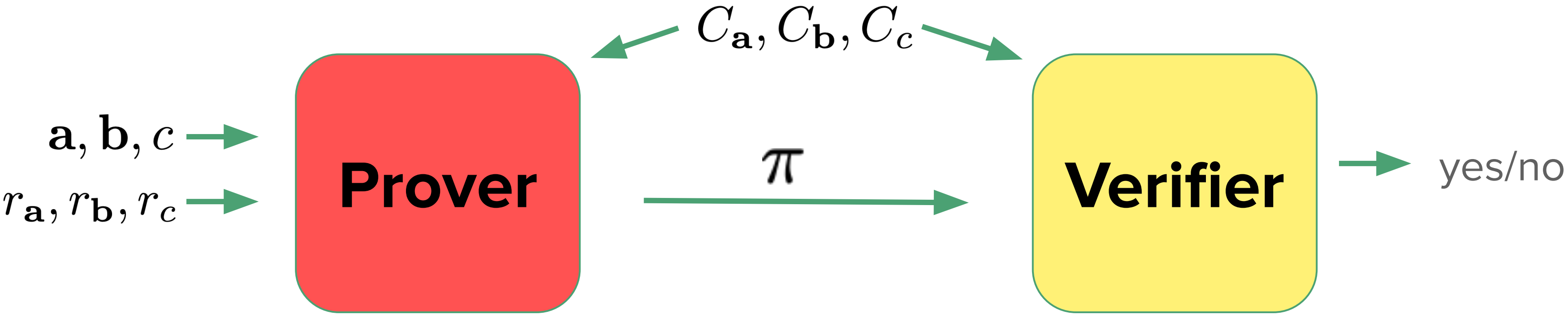
"I can open the given commitments to values such that they satisfy the inner product relation."

Zero-knowledge

Commit and Proof Systems

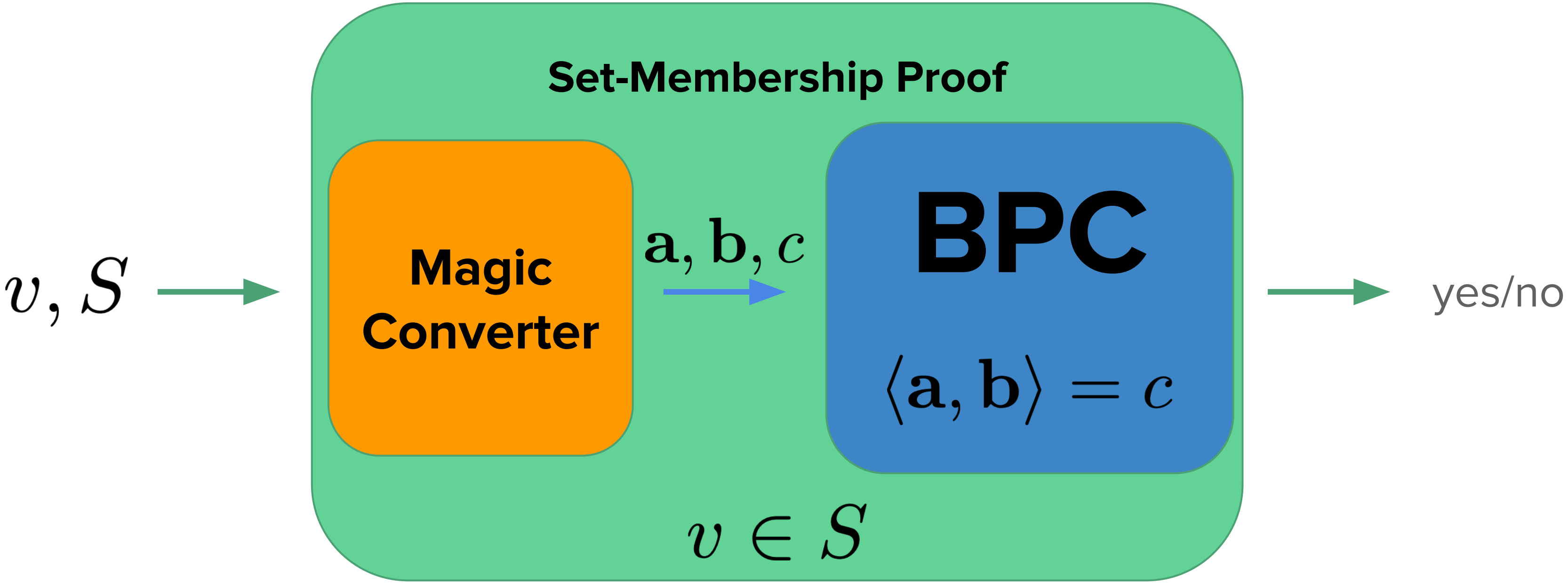
Non-Interactive





"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

$$\begin{matrix} v, S \\ v \in S \end{matrix} \longrightarrow \boxed{\textbf{Magic Converter}} \longrightarrow \begin{matrix} \mathbf{a}, \mathbf{b}, c \\ \langle \mathbf{a}, \mathbf{b} \rangle = c \end{matrix}$$

$$S$$

$$C_v \longrightarrow C_{\mathbf{a}}, C_{\mathbf{b}}, C_c$$

$$v, r_v \longrightarrow \mathbf{a}, \mathbf{b}, c \quad r_{\mathbf{a}}, r_{\mathbf{b}}, r_c$$

Polynomials

This is where X comes into play

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

Number

Finding ~~Nemo~~ Roots

$$P(X) = 0$$

Unless P is zero-polynomial

There are at most n roots.

Example

$$X^2 - 4$$

2 is a root

Coefficients Vector

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

A very large number (mod q)

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

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

$$\mathbf{a} = \mathbf{0} \quad \xrightarrow{\textbf{S.Z.}} \quad \langle \mathbf{a}, \mathbf{y}^n \rangle = 0 \qquad \mathbf{y^n} = \begin{pmatrix} 1 \\ \vdots \\ y^{n-1} \end{pmatrix}$$

Polynomial evaluation at y

Set-membership Proof

Set-Membership - Reduction to Inner Product

$$v \in S = \{s_1, \ldots, s_n\} \qquad v = s_i$$

"I know v is in S"

Vectorize

at position i

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

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

"I know the index i such that v = si"

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

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

public

secret ➔ untrusted

at position i

Consistency checks for a_L // zero vector with exactly one 1

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

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

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

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

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

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

Equations:

$$\begin{aligned} \langle \mathbf{s}, \mathbf{a}_L \rangle &= v \\ \langle \mathbf{a}_L, \mathbf{1} \rangle &= 1 \\ \mathbf{a}_L \circ \mathbf{a}_R &= \mathbf{0} \\ (\mathbf{a}_L - \mathbf{1}) - \mathbf{a}_R &= \mathbf{0} \end{aligned}$$

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

S.Z.

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

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

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

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

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

S.Z.

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

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

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

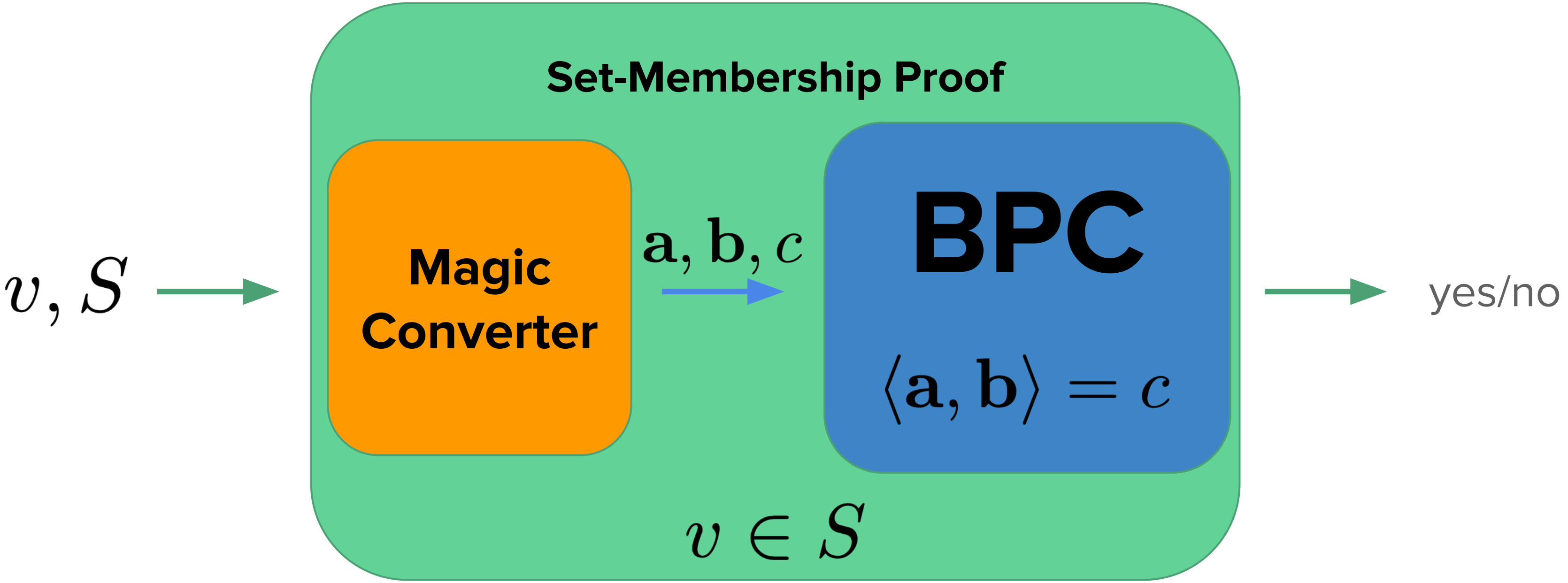
$$z^3 + z^2 v = z^3 \langle \mathbf{a}_L, \mathbf{1} \rangle + z^2 \langle \mathbf{a}_L, \mathbf{s} \rangle + z \langle \mathbf{a}_L - \mathbf{1} - \mathbf{a}_R, \mathbf{y}^n \rangle + \langle \mathbf{a}_L, \mathbf{a}_R \circ \mathbf{y}^n \rangle$$

Rewriting the equation in a clever way

public function

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

Set-membership - Construction Idea



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

Set-Non-Membership

$v \notin S = \{s_1, \ldots, s_n\}$ *"I know v is not in S"*

$\Leftrightarrow$

$\forall i \quad v \neq s_i$ *"I know v is not si for any i"*

$\Leftrightarrow$

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

$\Leftrightarrow$ Finite field

$\forall i \; \exists a_i \quad a_i(v - s_i) = 1$ *"I know the multiplicative inverse of (v-si) for any i"*

Set-Non-Membership

$v \notin S = \{s_1, \ldots, s_n\}$ *"I know v is not in S"*

$\Leftrightarrow$

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

$$\begin{aligned} \mathbf{a}_L \circ (\mathbf{a}_R - \mathbf{s}) &= \mathbf{1}, \\ \mathbf{a}_R &= v\mathbf{1}. \end{aligned}$$