ZKBOO

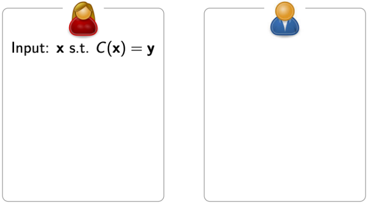
Table of Contents

MPC

Definition

Σ-Protocol

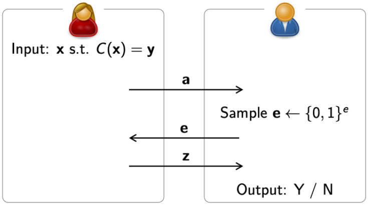
Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



Definition

Σ-Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



Definition

Σ-Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$

Input: $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{y}$

$\xrightarrow{\mathbf{a}}$

Sample $\mathbf{e} \leftarrow \{0,1\}^e$

$\xleftarrow{\mathbf{e}}$

$\xrightarrow{\mathbf{z}}$

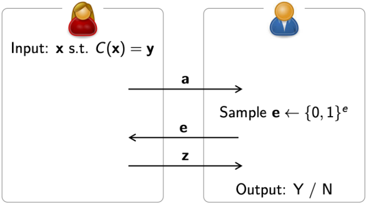
Output: Y / N

Complete: if Alice and Bob honest and $C(\mathbf{x}) = \mathbf{y}$,
$\Pr[\text{Bob outputs Y}] = 1$

Definition

Σ-Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



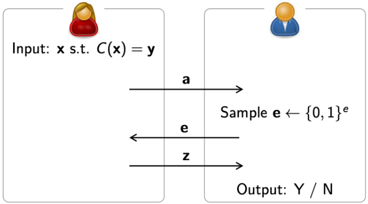
Soundness: from ≥ 2 accepting conversations $(\mathbf{a}, \mathbf{e}_i, \mathbf{z}_i)$ with $\mathbf{e}_i \neq \mathbf{e}_j$ we can efficiently compute $\mathbf{x}'$ s.t. $C(\mathbf{x}') = \mathbf{y}$

7 / 15

Definition

Σ-Protocol

Public data: $C : \{0,1\}^n \rightarrow \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$

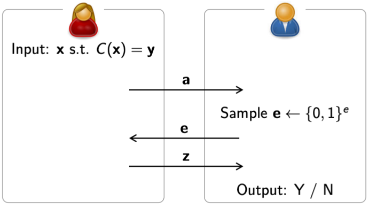


The protocol has **soundness error** ϵ:
if Alice is cheating, then Pr[Bob outputs Y] $\leq \epsilon$

Definition

Σ-Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$

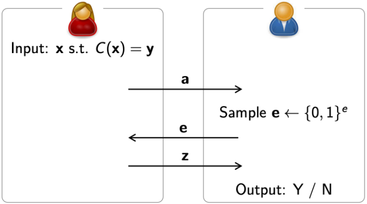


(Honest-Verifier) **ZK property**:
the distribution of $(\mathbf{a}, \mathbf{e}, \mathbf{z})$ does not reveal info on $\mathbf{x}$

Definition

Σ-Protocol

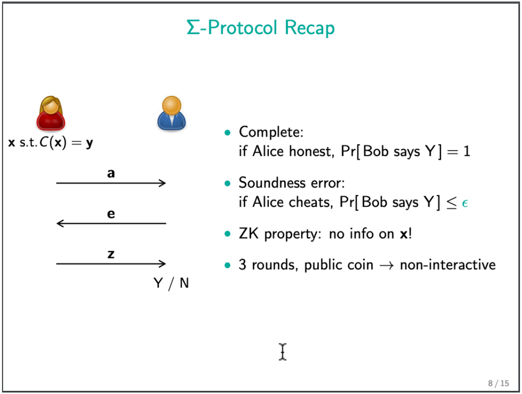
Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



It can be made non-interactive!
(Fiat-Shamir heuristic)

7 / 15

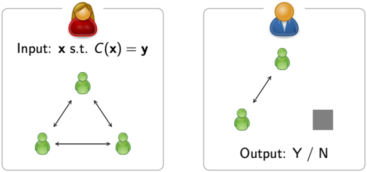
Definition


Σ-Protocol Recap
x s.t. C(x) = y
a
e
z
Y / N
Complete:
if Alice honest, Pr[Bob says Y] = 1
Soundness error:
if Alice cheats, Pr[Bob says Y] ≤ ϵ
ZK property: no info on x!
3 rounds, public coin → non-interactive
8 / 15

Definition

Related work:

IKOS Construction
(or “MPC-in-the-head”)
[Ishai-Kushilevitz-Ostrovsky-Sahai 2007]



9 / 15

Definition

Circuit decomposition:

Goal: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

10 / 15

Definition

Circuit decomposition:

Goal: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

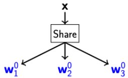
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and

$$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$$

Definition

Circuit decomposition:



Goal: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

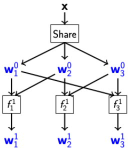
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and
$$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$$

10 / 15

Definition

Circuit decomposition:



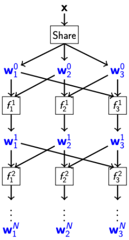
<u>Goal</u>: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

Let N be a fixed integer, consider the following finite set of functions:

$$\boxed{\text{Share, Rec and} \quad \mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\ldots,N}}$$

Definition

Circuit decomposition:



Goal: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

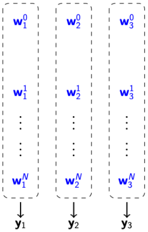
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and

$$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$$

Definition

Circuit decomposition:



Goal: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

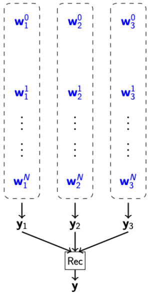
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and
$$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$$

10 / 15

Definition

Circuit decomposition:



<u>Goal</u>: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

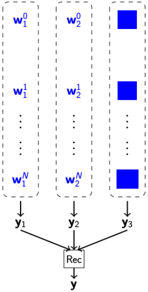
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and
$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$

- correctness: $\mathbf{y} = C(\mathbf{x})$

Definition

Circuit decomposition:



<u>Goal</u>: compute $C(\mathbf{x})$ splitting the computation in 3 branches s.t. looking at any 2 consecutive branches gives no info on $\mathbf{x}$

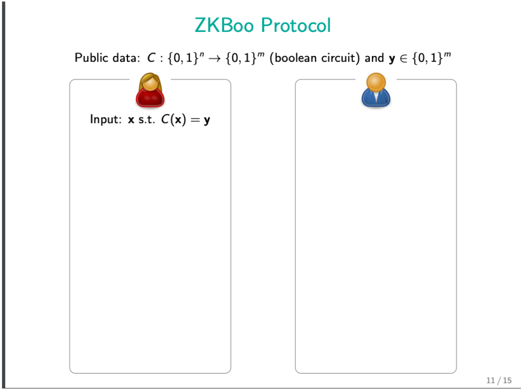
Let N be a fixed integer, consider the following finite set of functions:

Share, Rec and
$$\mathcal{F} = \{f_1^{(j)}, f_2^{(j)}, f_3^{(j)}\}_{j=1,\dots,N}$$

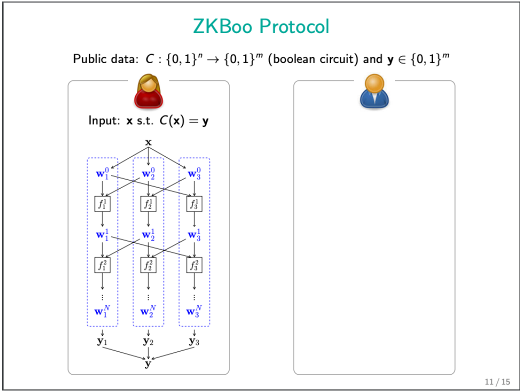
- correctness: $\mathbf{y} = C(\mathbf{x})$
- 2-privacy: $\forall\, e, \forall\, j\ (\mathbf{w}_e^j, \mathbf{w}j_{e+1}, \mathbf{y}_{e+2})$ doesn't reveal info on $\mathbf{x}$

10 / 15

Definition


ZKBoo Protocol
Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$
Input: $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{y}$
11 / 15

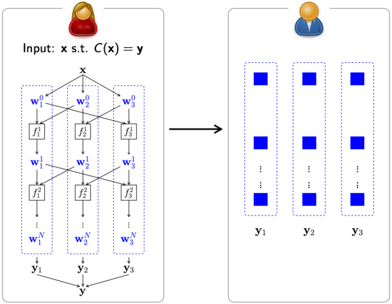
Definition


ZKBoo Protocol
Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$
Input: $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{y}$
$\mathbf{x}$
$\mathbf{w}_1^0$ $\mathbf{w}_2^0$ $\mathbf{w}_3^0$
f_1^1 f_2^1 f_3^1
$\mathbf{w}_1^1$ $\mathbf{w}_2^1$ $\mathbf{w}_3^1$
f_1^2 f_2^2 f_3^2
$\mathbf{w}_1^N$ $\mathbf{w}_2^N$ $\mathbf{w}_3^N$
$\mathbf{y}_1$ $\mathbf{y}_2$ $\mathbf{y}_3$
$\mathbf{y}$
11 / 15

Definition

ZKBoo Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$

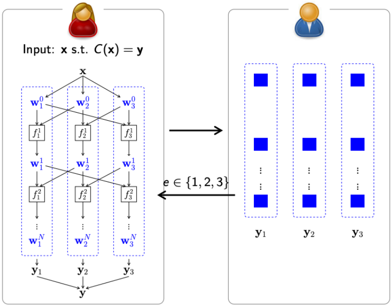


11 / 15

Definition

ZKBoo Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$

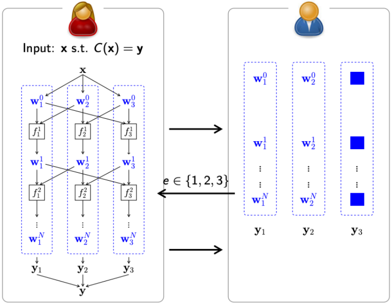


11 / 15

Definition

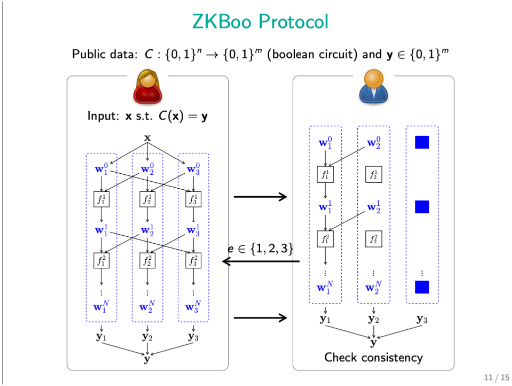
ZKBoo Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



11 / 15

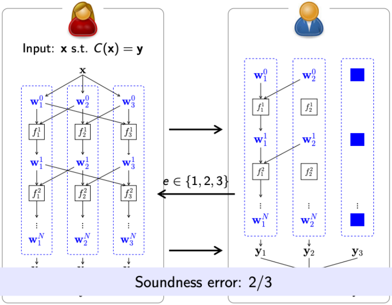
Definition


ZKBoo Protocol
Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$
Input: $\mathbf{x}$ s.t. $C(\mathbf{x}) = \mathbf{y}$
$e \in \{1,2,3\}$
Check consistency
11 / 15

Definition

ZKBoo Protocol

Public data: $C : \{0,1\}^n \to \{0,1\}^m$ (boolean circuit) and $\mathbf{y} \in \{0,1\}^m$



Soundness error: 2/3