Composition of Zero-Knowledge Proofs with Efficient Provers

Eleanor Birrell Salil Vadhan

Cornell University Harvard University

February 11, 2010

Motivation

- Reducing Error

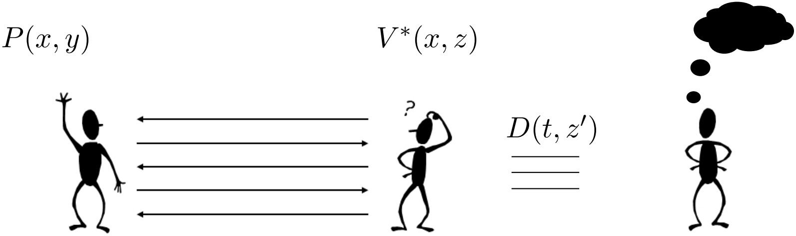
Motivation

- Reducing Error
- Networked Environments

Motivation

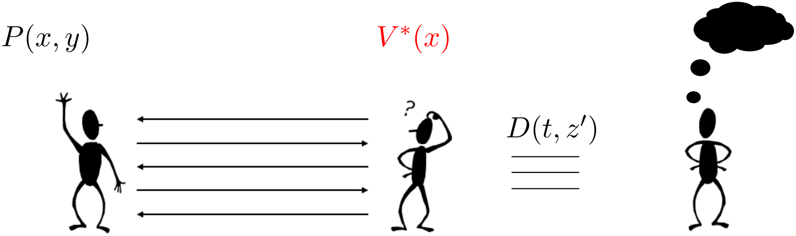
- Reducing Error
- Networked Environments
- Composibility is subtle – definitions matter (e.g., Efficient Provers)

Defining Zero Knowledge



Auxiliary-input ZK

Defining Zero Knowledge

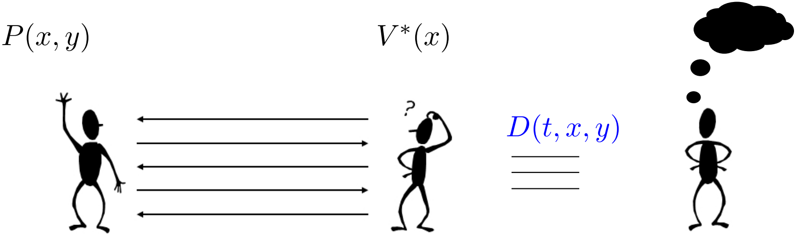


Auxiliary-input ZK

Plain ZK [GMR]

- Nonuniform ZK: $D(t, z')$

Defining Zero Knowledge

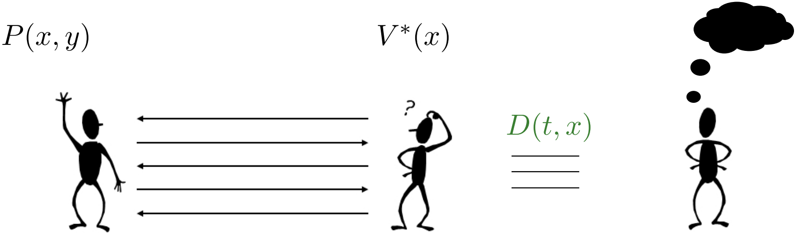


Auxiliary-input ZK

Plain ZK [GMR]

- Nonuniform ZK: $D(t, z')$
- P-uniform ZK: $D(t, x, y)$

Defining Zero Knowledge



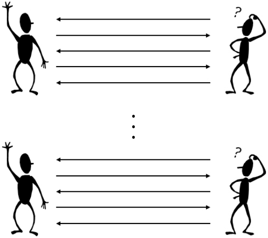
Auxiliary-input ZK

Plain ZK [GMR]

- Nonuniform ZK: $D(t, z')$
- P-uniform ZK: $D(t, x, y)$
- V-uniform ZK: $D(t, x)$

Composition

- Sequential Composition:



- Parallel Composition:

Sequential Composition: Previous Results

- Goldreich-Krawczyk '90: Nonuniform Plain ZK is not 2-composable.

Sequential Composition: Previous Results

- Goldreich-Krawczyk '90: Nonuniform Plain ZK is not 2-composable.
- Goldreich-Oren '94: Auxiliary-input ZK is closed under polynomial composition.

Sequential Composition: Previous Results

Sequential Composition of Plain ZK:

	P-/Non-uniform ZK	V-Uniform ZK
Efficient Prover	??	??
Unbounded Prover	Not 2-comp [GK]	Not 2-comp [GK]

Efficient $=$ P poly-time given input x and witness y

Sequential Composition: Our Results

Sequential Composition of Plain ZK:

	P-/Non-uniform ZK	V-Uniform ZK
Efficient Prover	$O(1)$-comp	
Unbounded Prover	Not 2-comp [GK]	Not 2-comp [GK]

Efficient $=$ P poly-time given input x and witness y

Sequential Composition: Our Results

Sequential Composition of Plain ZK:

	P-/Non-uniform ZK	V-Uniform ZK
Efficient Prover	$O(1)$-comp	Not 2-comp
Unbounded Prover	Not 2-comp [GK]	Not 2-comp [GK]

Efficient $=$ P poly-time given input x and witness y

Parallel Composition: Previous Results

- Feige-Shamir '90: DL hard $\Rightarrow$ Efficient-prover auxiliary-input ZK is not 2-composable in parallel.

Parallel Composition: Previous Results

- Feige-Shamir '90: DL hard $\Rightarrow$ Efficient-prover auxiliary-input ZK is not 2-composable in parallel.
- Feige-Shamir '90: $\mathcal{UP} \not\subseteq \mathcal{BPP}$ and OWF $\Rightarrow$ Efficient-prover auxiliary-input ZK is not 2-composable in parallel.

Parallel Composition: Previous Results

- Feige-Shamir '90: DL hard $\Rightarrow$ Efficient-prover auxiliary-input ZK is not 2-composable in parallel.
- Feige-Shamir '90: $\mathcal{UP} \not\subseteq \mathcal{BPP}$ and OWF $\Rightarrow$ Efficient-prover auxiliary-input ZK is not 2-composable in parallel.
- Goldriech-Krawczyk '90: Unbounded-prover auxiliary-input ZK is not 2-composable in parallel.

Parallel Composition: Previous Results

Parallel Composition of Auxiliary-input ZK:

	Auxiliary-input ZK
Efficient Prover	DL $\Rightarrow$ not 2-comp [FS] $\mathcal{UP} \not\subseteq \mathcal{BPP}$ + OWF $\Rightarrow$ not 2-comp [FS]
Unbounded Prover	Not 2-comp [GK]

Parallel Composition: Our Results

Parallel Composition of Auxiliary-input ZK:

	Auxiliary-input ZK
Efficient Prover	DL $\Rightarrow$ not 2-comp [FS] $\mathcal{UP} \not\subseteq \mathcal{BPP}$ + OWF $\Rightarrow$ not 2-comp [FS] key agreement* $\Rightarrow$ not 2-comp
Unbounded Prover	Not 2-comp [GK]

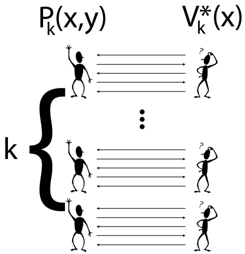
Nonuniform (resp. P-Uniform) Sequential Result

	P-/Non-uniform ZK	V-Uniform ZK
Efficient Prover	$O(1)$-comp	Not 2-comp
Unbounded Prover	Not 2-comp [GK]	Not 2-comp [GK]

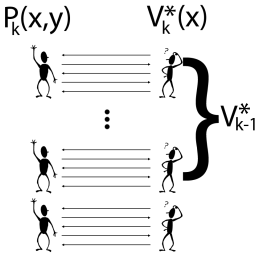
Theorem

Efficient-prover P-uniform plain ZK is closed under $O(1)$-sequential composition.

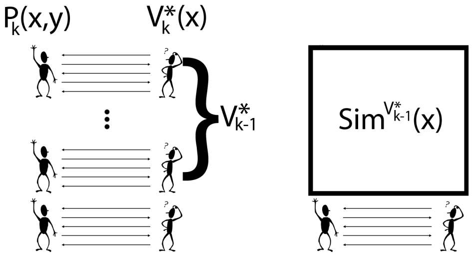
Proof of Nonuniform (resp. P-Uniform) Result



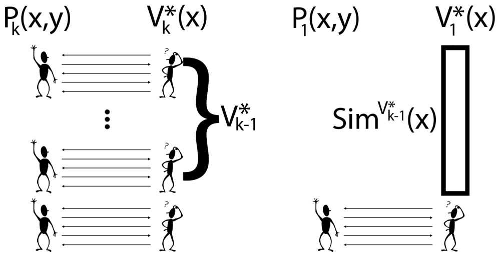
Proof of Nonuniform (resp. P-Uniform) Result



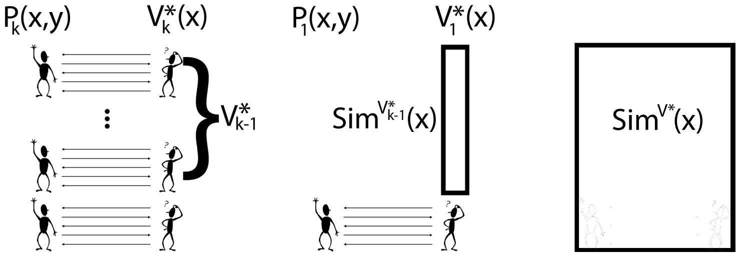
Proof of Nonuniform (resp. P-Uniform) Result



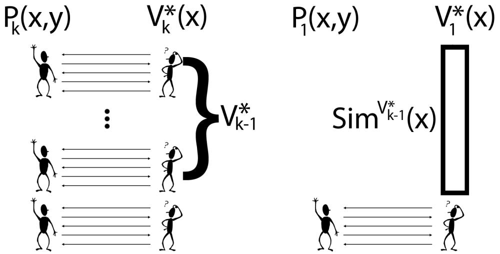
Proof of Nonuniform (resp. P-Uniform) Result



Proof of Nonuniform (resp. P-Uniform) Result

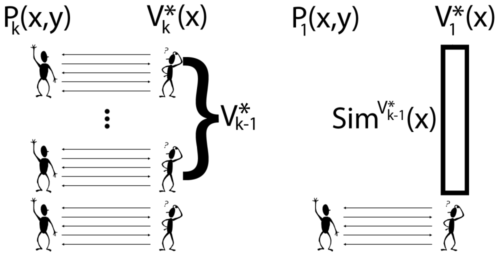


Proof of Nonuniform (resp. P-Uniform) Result



$D(x, y, t_k)$

Proof of Nonuniform (resp. P-Uniform) Result



$D(x, y, t_k)$

$D'(x, y, t_{k-1}) = D(x, y, f(x, y, t_{k-1}))$

V-Uniform Sequential Result

	P-/Non-uniform ZK	V-Uniform ZK
Efficient Prover	$O(1)$-comp	Not 2-comp
Unbounded Prover	Not 2-comp [GK]	Not 2-comp [GK]

Theorem

Efficient-prover V-uniform plain ZK is not 2-composable.

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

Definition (Evasive Pseudorandom Ensemble)

$S_1, S_2, \ldots$

- $S_m \subseteq \{0,1\}^m$
- $S_m \overset{c}{\equiv} U_m$
- hard to generate elements of S_m.

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\stackrel{s}{\leftarrow}$	$s \in_R \{0,1\}^{4n}$

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = K(x)$		
	else $c \in_R S_{4n}$	$\xrightarrow{c}$	

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\overset{s}{\longleftarrow}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = K(x)$		
	else $c \in_R S_{4n}$	$\overset{c}{\longrightarrow}$	

2. Sequential Composition of two copies:

Step	$P(x)$		$V(x)$
1		$\overset{s}{\longleftarrow}$	$s \in_R \{0,1\}^{4n}$

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\overset{s}{\longleftarrow}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = K(x)$		
	else $c \in_R S_{4n}$	$\overset{c}{\longrightarrow}$	

2. Sequential Composition of two copies:

Step	$P(x)$		$V(x)$
1		$\overset{s}{\longleftarrow}$	$s \in_R \{0,1\}^{4n}$
2	$c \in_R S_{4n}$	$\overset{c}{\longrightarrow}$	

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = K(x)$		
	else $c \in_R S_{4n}$	$\xrightarrow{c}$	

2. Sequential Composition of two copies:

Step	$P(x)$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	$c \in_R S_{4n}$	$\xrightarrow{c}$	
1		$\xleftarrow{s}$	$s = c$

Overview of Goldreich-Krawczyk Construction (Unbounded Prover)

1. Single protocol:

Step	$P(x)$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = K(x)$		
	else $c \in_R S_{4n}$	$\xrightarrow{c}$	

2. Sequential Composition of two copies:

Step	$P(x)$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	$c \in_R S_{4n}$	$\xrightarrow{c}$	
1		$\xleftarrow{s}$	$s = c$
2	since $s \in S_{4n}$: $c = K(x)$	$\xrightarrow{c}$	

Proof of V-Uniform Result

Definition (Efficient Evasive Pseudorandom Ensemble)

$S_1, S_2, \ldots$

- $S_m \subseteq \{0,1\}^m$
- Machines with $\leq m/4$ bits of advice:
  - $S_m \stackrel{c}{\equiv} U_m$
  - hard to generate elements of S_m.
- $\exists$ an advice string π_m of length $\mathsf{poly}(m)$ s.t. efficient machines with this advice can:
  - Check membership
  - Generate uniformly random elements

Proof of V-Uniform Result

Definition (Efficient Evasive Pseudorandom Ensemble)

$S_1, S_2, \ldots$

- $S_m \subseteq \{0,1\}^m$
- Machines with $\leq m/4$ bits of advice:
  - $S_m \stackrel{c}{\equiv} U_m$
  - hard to generate elements of S_m.
- $\exists$ an advice string π_m of length $\mathsf{poly}(m)$ s.t. efficient machines with this advice can:
  - Check membership
  - Generate uniformly random elements

Construction: pairwise independent family:

$$h_m \in_R \mathcal{H}_{m,k} = \{h_{m,k}(x) = ax + b|_k\}$$

Proof of V-Uniform Result

Definition (Efficient Evasive Pseudorandom Ensemble)

$S_1, S_2, \ldots$

- $S_m \subseteq \{0,1\}^m$
- Machines with $\leq m/4$ bits of advice:
  - $S_m \overset{c}{\equiv} U_m$
  - hard to generate elements of S_m.
- $\exists$ an advice string π_m of length $\mathsf{poly}(m)$ s.t. efficient machines with this advice can:
  - Check membership
  - Generate uniformly random elements

Construction: pairwise independent family:

$$h_m \in_R \mathcal{H}_{m,k} = \{h_{m,k}(x) = ax + b|_k\}$$
$$S_m = \{x \in \{0,1\}^m : h_m(x) = 0^k\},\ \pi_m = (a,b).$$

Proof of V-Uniform Result

1. Single protocol:

Step	$P(x, \pi_{4n})$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	if $s \in S_{4n}$: $c = w$		
	else $c \in_R S_{4n}$	$\xrightarrow{c}$	

2. Sequential Composition of two copies:

Step	$P(x, \pi_{4n})$		$V(x)$
1		$\xleftarrow{s}$	$s \in_R \{0,1\}^{4n}$
2	$c \in_R S_{4n}$	$\xrightarrow{c}$	
1		$\xleftarrow{s}$	$s = c$
2	since $s \in S_{4n}$: $c = w$	$\xrightarrow{c}$	

Conclusions

Highlight impact of efficient provers

Conclusions

Highlight impact of efficient provers

Questions?