On the Amortized Complexity of Zero Knowledge Protocols for Multiplicative Relations

Ronald Cramer[1] Ivan Damgård[2] Valerio Pastro[2]

[1]CWI Amsterdam

[2]Aarhus University

August 15, 2012

The Problem

Scenario

- P holds x, y, z (in a finite field K) s.t. $z = xy$
- V holds hom. commitments $com(x), com(y), com(z)$, of size κ
- V wants to be sure $z = xy$
- P does not want to reveal x, y, z

Commitments

Homomorphic: $com(a) \cdot com(b) = com(a + b)$

Shorthand: $com(\cdot) = [\cdot]$

The Problem

Motivation

- Zero Knowledge proofs for satisfiability of Boolean circuits
- MPC based on additive secret sharing [BDOZ11, DPSZ12]
- Anonymous credentials, group signatures, ...

Previous and Related Work (Apologies if I forgot any of your papers)

1991	Beaver	[Bea91]
1997	Fujisaki, Okamoto	[FO97]
1999	Cramer et al.,	[CDD+99]
2002	Damgård, Fujisaki	[DF02]
2009	Cramer, Damgård	[CD09]
2012	Ben-Sasson et al.	[BSFO12]

A Well-Known Solution [Bea91]

Protocol

- P samples uniform $a, b \leftarrow K$
- P computes $c = ab$, and sends $[a], [b], [c]$ to V
- V sends a uniform $e \leftarrow K$
- P opens $[ex - a], [y - b]$, define $\varepsilon := ex - a, \delta := y - b$
- P opens $[ez - c - \varepsilon b - \delta a - \varepsilon\delta]$
- V checks that P opened to 0

Properties

Correctness:	P honest	$\Longrightarrow$	$ez - c - \varepsilon b - \delta a - \varepsilon\delta = 0$	
Soundness:	P dishonest	$\Longrightarrow$	Cheat with prob $1/\lvert K \rvert$	(guess e)

Room for Improvement

What if $|K|$ small (e.g. $K = \mathbb{F}_2$)?

Constant soundness error probability $\Longrightarrow$ Bad!

Repeating l times $\Longrightarrow$ soundness error 2^{-l}

Communication? $O(\kappa \cdot l)$

Basic Field Case

	Soundness Error	Amortized comm. complexity
Previous solutions:	2^{-l}	$O(l \cdot \kappa)$
Our work:	2^{-l}	$O(\kappa)$

Our Solution

Ingredients

- Homomorphic commitments (size $= \kappa$)
  (for this part:
  statistically binding, computationally hiding commitment schemes)
- Linear (multi)secret sharing schemes with R-product reconstruction
  (share s, share s',
  reconstruct $s \cdot s'$ as linear combo of shares of R players)

commitments:	not to reveal x, y, z
homomorphic:	to compute sums on committed values!
multi-secret:	to use amortization techniques! [CD09].

Amortization: more instances to prove $\Rightarrow$ better comm. complexity!

Digression on LSSS (multi-secret variant of Shamir)

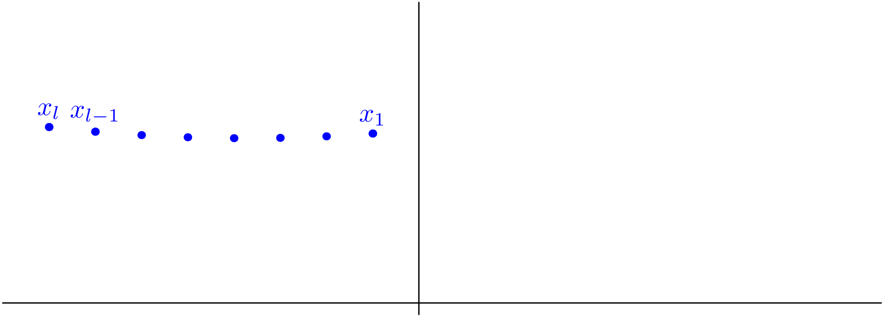
How to Share?

Secret: $\mathbf{x} := (x_1, \ldots, x_l)$.

Polynomial: $f_x \leftarrow K[X]$, with $\deg(f_x) = t + l$

$f_x(-i) = x_i$ for $i = 1, \ldots, l$

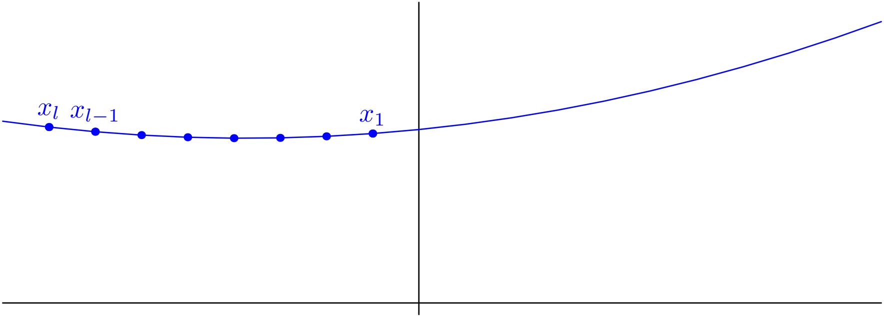
Shares: $f_x(1), \ldots, f_x(n)$



Digression on LSSS (multi-secret variant of Shamir)

How to Share?

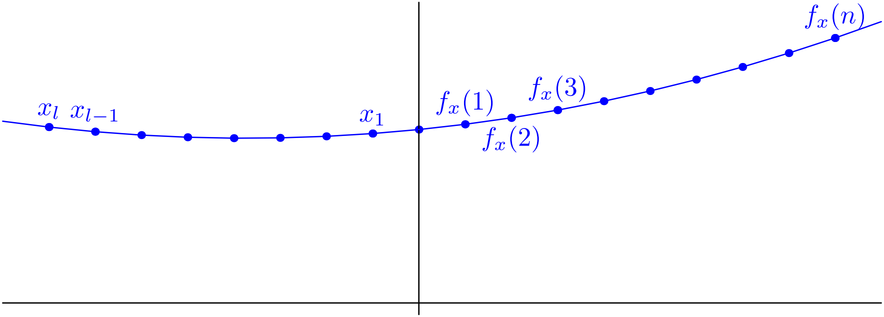
Secret:	$\mathbf{x} := (x_1, \ldots, x_l)$.
Polynomial:	$f_x \leftarrow K[X]$, with $\deg(f_x) = t + l$
	$f_x(-i) = x_i$ for $i = 1, \ldots, l$
Shares:	$f_x(1), \ldots, f_x(n)$



Digression on LSSS (multi-secret variant of Shamir)

How to Share?

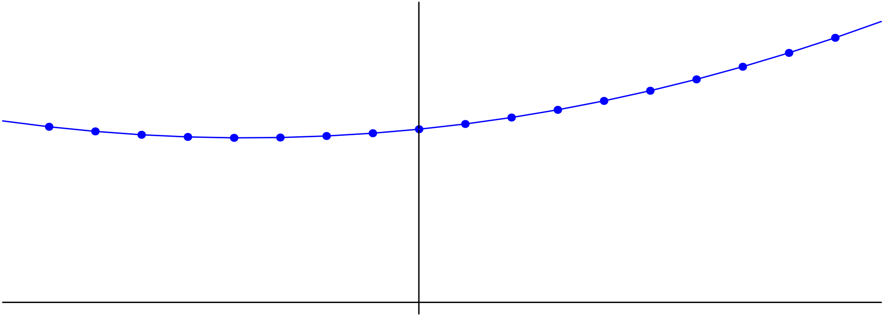
Secret:	$\mathbf{x} := (x_1, \ldots, x_l)$.
Polynomial:	$f_x \leftarrow K[X]$, with $\deg(f_x) = t + l$
	$f_x(-i) = x_i$ for $i = 1, \ldots, l$
Shares:	$f_x(1), \ldots, f_x(n)$



Digression on LSSS

Product Reconstruction? (Yes, if $n > 2(t+l)$)

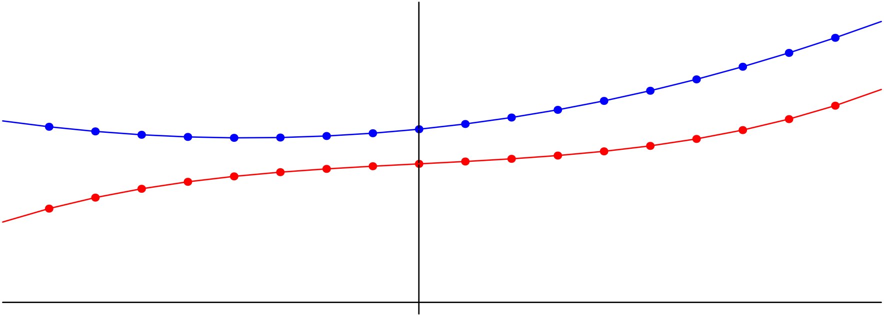
- Share $\mathbf{x}, \mathbf{y}$
- Local products $f_x(i) \cdot f_y(i)$ for $> 2(t+l)$ i's
- Reconstruct $f_x \cdot f_y$
- Evaluate $(f_x \cdot f_y)(-i)$ for $i = 1, \ldots, l$



Digression on LSSS

Product Reconstruction? (Yes, if $n > 2(t+l)$)

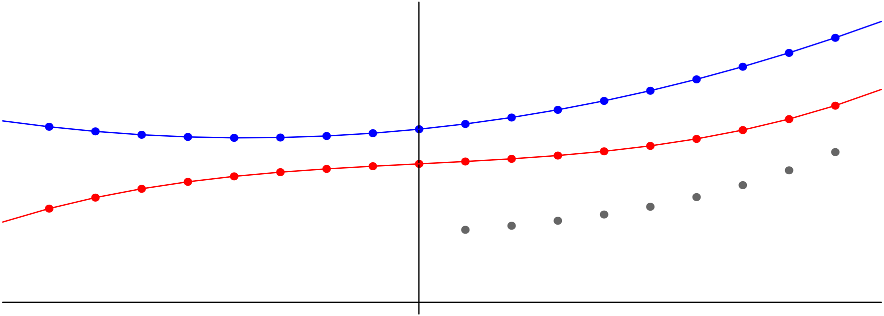
- Share $\mathbf{x}, \mathbf{y}$
- Local products $f_x(i) \cdot f_y(i)$ for $> 2(t+l)$ i's
- Reconstruct $f_x \cdot f_y$
- Evaluate $(f_x \cdot f_y)(-i)$ for $i = 1, \ldots, l$



Digression on LSSS

Product Reconstruction? (Yes, if $n > 2(t + l)$)

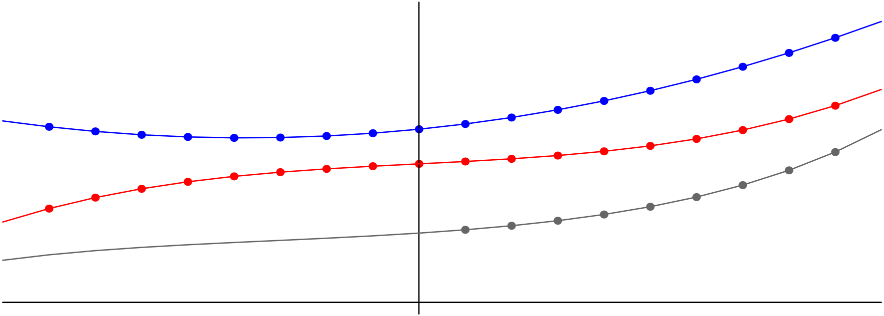
- Share $\mathbf{x}, \mathbf{y}$
- Local products $f_x(i) \cdot f_y(i)$ for $> 2(t + l)$ i's
- Reconstruct $f_x \cdot f_y$
- Evaluate $(f_x \cdot f_y)(-i)$ for $i = 1, \ldots, l$



Digression on LSSS

Product Reconstruction? (Yes, if $n > 2(t + l)$)

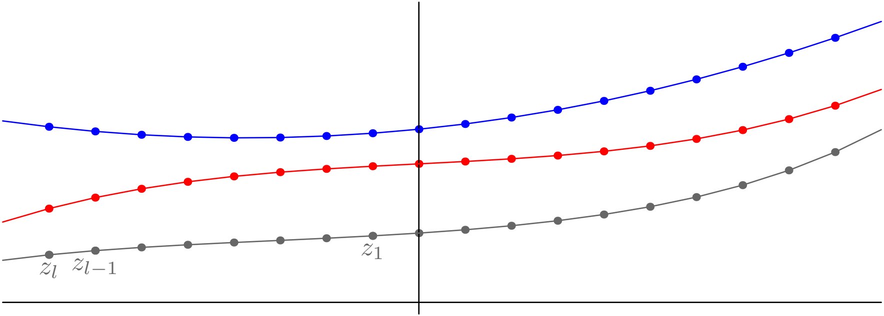
- Share $\mathbf{x}, \mathbf{y}$
- Local products $f_x(i) \cdot f_y(i)$ for $> 2(t + l)$ i's
- Reconstruct $f_x \cdot f_y$
- Evaluate $(f_x \cdot f_y)(-i)$ for $i = 1, \ldots, l$



Digression on LSSS

Product Reconstruction? (Yes, if $n > 2(t+l)$)

- Share $\mathbf{x}, \mathbf{y}$
- Local products $f_x(i) \cdot f_y(i)$ for $> 2(t+l)$ i's
- Reconstruct $f_x \cdot f_y$
- Evaluate $(f_x \cdot f_y)(-i)$ for $i = 1, \ldots, l$



Notice:

Fact #1

V holds t evals $f_x(j)$ and $f_y(j)$
$\Longrightarrow$ no info on $f_y(-i)$, $f_y(-i)$, $(f_x \cdot f_y)(-i)$ revealed to V.

Fact #2

$f \neq g \in K[X]$,
$\deg(f) = 2(t + l) = \deg(g)$
$\Longrightarrow$ f and g agree on at most $2(t + l)$ points.

Back to the Original Problem. What if . . . ?

Toy Protocol – Basic Field Scenario

- P samples $f_x, f_y \leftarrow K[X]$, with $\deg(f_x) = t + l = \deg(f_y)$, $f_x(-i) = x_i$, $f_y(-i) = y_i$
- P computes $f_z = f_x \cdot f_y$
- P commits $[f_x], [f_y], [f_z]$
- V chooses t indices $O \subset \{1, \dots, n\}$
- P opens $[f_x](j)$, $[f_y](j)$, $[f_z](j)$ for $j \in O$
- V accepts iff $f_x(j) \cdot f_y(j) = f_z(j)$

Private x_i, y_i, z_i

Fact $\#1 \Rightarrow$ no info revealed on secrets!

Soundness Error

Fact $\#2$ & Choice of $O \Rightarrow$ soundness error $\leq \left(\frac{2(t+l)}{n}\right)^t$

Back to the Original Problem. What if . . . ?

Toy Protocol – Basic Field Scenario

- P samples $f_x, f_y \leftarrow K[X]$, with $\deg(f_x) = t + l = \deg(f_y)$, $f_x(-i) = x_i$, $f_y(-i) = y_i$
- P computes $f_z = f_x \cdot f_y$
- P commits $[f_x], [f_y], [f_z]$
- V chooses t indices $O \subset \{1, \ldots, n\}$
- P opens $[f_x](j)$, $[f_y](j)$, $[f_z](j)$ for $j \in O$
- V accepts iff $f_x(j) \cdot f_y(j) = f_z(j)$

Private x_i, y_i, z_i

Fact $\#1 \Rightarrow$ no info revealed on secrets!

Soundness Error

Fact $\#2$ & Choice of $O \Rightarrow$ s.e. $\leq \left(\frac{2(t+l)}{n}\right)^t = 2^{-l}$, if $t, l = \Theta(n)$

The General Result

Shamir: $n < |K| \Longrightarrow$ general LSSS?

Basic Field Case

Using a linear (multi)secret sharing scheme over K with

- K a finite field
- d players
- t privacy
- l secrets
- R product reconstruction

A zero-knowledge protocol for the language

$$\left\{ (com(x_i), com(y_i), com(z_i))_{i=1}^{l} \mid x_i, y_i, z_i \in K; x_i \cdot y_i = z_i \right\},$$

with soundness error $\left(\frac{R-1}{d}\right)^t$

Parameters

Choice of parameters to get negligible soundness error:

Basic Field Case

Using a linear (multi)secret sharing scheme over K with

- K a finite field
- d players $d = \Theta(l)$
- t privacy $t = \Theta(l)$
- l secrets
- R product reconstruction $R = \Theta(l)$

A zero-knowledge protocol for the language

$$\left\{ (com(x_i), com(y_i), com(z_i))_{i=1}^{l} \mid x_i, y_i, z_i \in K; x_i \cdot y_i = z_i \right\},$$

with soundness error $\left(\frac{R-1}{d}\right)^t = 2^{-l}$. Amo.Comm.: $O(\kappa)$

Comparisons & Extensions

Basic Field Case

	Soundness Error	Amortized comm. complexity
Our work:	2^{-l}	$O(\kappa)$
Previous solutions:	2^{-l}	$O(l \cdot \kappa)$

Let's play!
What if values were integers (rather than in a finite field)?
We have a solution!

k-bit Integers Case

	Security Notion
Our work:	Factoring
Previous solutions:	Strong-RSA

Comparisons & Extensions - General Field Case

Basic field case: $x \cdot y = z.$
General field case: $D(x_1, \ldots, x_v) = z.$

Extension of protocol: to prove *any* algebraic rel. on committed values.
Formally, a zero knowledge protocol for the language

$$\Big\{(com(x_{1,i}), \ldots, com(x_{v,i}), com(z_i))_{i=1}^{l} \mid x_{1,i}, \ldots, x_{v,i}, z_i \in K; D(x_{1,i}, \ldots, x_{v,i}) = z_i\Big\},$$

where D is an algebraic circuit.

Final Slide

Q: Standard commitments: cheating?

A: We also consider commitments of the following form

$$[v] : \begin{cases} P & : \quad v, \quad m_v = a \cdot v + b_v \\ V & : \quad a, \quad b_v \end{cases}$$

given by some setup,
e.g. the preprocessing phase of [BDOZ11], or [DPSZ12].

Such commitments:

- Homomorphic (that is all we need!)
- Information theoretically secure
- NEW! Can be used over the integers!

Final Slide

Q: Standard commitments: cheating?

A: We also consider commitments of the following form

$$[v] : \begin{cases} P & : \quad v, \quad m_v = a \cdot v + b_v \\ V & : \quad a, \quad b_v \end{cases}$$

given by some setup,
e.g. the preprocessing phase of [BDOZ11], or [DPSZ12].

Such commitments:

- Homomorphic (that is all we need!)
- Information theoretically secure
- NEW! Can be used over the integers!

Thanks! — Merci!

Rikke Bendlin, Ivan Damgård, Claudio Orlandi, and Sarah Zakarias.
Semi-homomorphic encryption and multiparty computation.
In *EUROCRYPT*, pages 169–188, 2011.

Donald Beaver.
Efficient multiparty protocols using circuit randomization.
In *CRYPTO*, pages 420–432, 1991.

Eli Ben-Sasson, Serge Fehr, and Rafail Ostrovsky.
Near-linear unconditionally-secure multiparty computation with a dishonest minority.
In *CRYPTO*, 2012.
To appear.

Ronald Cramer and Ivan Damgård.
On the amortized complexity of zero-knowledge protocols.
In Shai Halevi, editor, *CRYPTO*, volume 5677 of *Lecture Notes in Computer Science*, pages 177–191. Springer, 2009.

Ronald Cramer, Ivan Damgård, Stefan Dziembowski, Martin Hirt, and Tal Rabin.

Efficient multiparty computations secure against an adaptive adversary.
In *EUROCRYPT*, pages 311–326, 1999.

Ivan Damgård and Eiichiro Fujisaki.
A statistically-hiding integer commitment scheme based on groups with hidden order.
In Yuliang Zheng, editor, *ASIACRYPT*, volume 2501 of *Lecture Notes in Computer Science*, pages 125–142. Springer, 2002.

Ivan Damgård, Valerio Pastro, Nigel P. Smart, and Sarah Zakarias.
Multiparty computation from somewhat homomorphic encryption.
In *CRYPTO*, 2012.
To appear.

Eiichiro Fujisaki and Tatsuaki Okamoto.
Statistical zero knowledge protocols to prove modular polynomial relations.
In Burton S. Kaliski Jr., editor, *CRYPTO*, volume 1294 of *Lecture Notes in Computer Science*, pages 16–30. Springer, 1997.