Additive Combinatorics and Discrete Logarithm Based Range Protocols

Rafik Chaabouni[1] Helger Lipmaa[2,3] abhi shelat[4]

[1]EPFL LASEC, Switzerland
[2]Cybernetica AS, Estonia
[3]Tallinn University, Estonia
[4]University of Virginia, USA

ACISP 2010 July 7, 2010

General Research Question: Range Proofs

New Efficient Protocol for Range Proofs

- Range (Interval) Proof

Public parameters: range $\Phi = [L, H)$ of integer elements,
$C = Com(x)$

Prover **Verifier**

$x \in \Phi$

$$\xrightarrow{PK\{x\ :\ C{=}Com(x)\ \wedge\ x{\in}\Phi\}}$$

- x must not be revealed (zero-knowledge)
- Honest Verifier Model (Malicious Verifier possible)
- Better Efficiency

  Practically Competitive

Introduction

Motivation

Community Interest

- Cryptography Primitives
- Credential Revocation (Freshness of a Token)
- Anonymous Credentials (Identity and Authentication Proofs)

Concrete Examples

- Strict age anonymity (e.g. under 26, but older than 18).
- e-voting protocols, e-auctions, etc.

Zero-Knowledge Proofs

- Full security of cryptographic protocols is often achieved by having a zero-knowledge proof (of knowledge).
- Zero-knowledge: does not leak any extra information
- Proof: the actions of any party are consistent with his committed input $Com(x)$
- We actually are interested in Σ-protocols (see the paper).

Homomorphic Commitments

- To construct *efficient* ZK proofs, one needs to assume that *Com* satisfies nice algebraic properties.
- Homomorphic commitment: $Com(x) \cdot Com(x') = Com(x + x')$.
- Then
$$Com(x)^a = \prod_a Com(x) = Com(ax).$$
- From this trivially,
$$\prod_i Com(x_i)^{a_i} = Com\left(\sum_i a_i x_i\right) \text{ for any integers } a_i.$$

Additive Combinatorics

- Define $A + B := \{a + b : a \in A \wedge b \in B\}$ and $b * A := \{ba : a \in A\}$.
- $A + B$ is a sumset, $b * A$ is b-dilate of A.
- *Additive combinatorics* is the subject that studies the properties of sumsets.

Previous Work
Background

Zero-Knowledge Proofs and Additive Combinatorics

- To prove that $C = Com(x) \land x \in \Phi$:
  - Set $C_i = Com(x_i)$ for some x_i.
  - ZK-prove that $C_i = Com(x_i) \land x_i \in \Phi_i$ for all i, where $\Phi = \sum b_i * \Phi_i$.
  - Compute $C = Com(x) = \prod Com(x_i)^{b_i}$.
- Requires:
  - Efficient sumset-presentation $\Phi = \sum_{i=0}^{\ell-1} b_i * \Phi_i$.
    $\Rightarrow \ell \ll n$ with n small.
  - Efficient ZK-proofs that $C_i = Com(x_i) \land x_i \in \Phi_i$.
    $\Rightarrow$ *small structured sets* Φ_i.

Folklore Bit Commitment

Folklore Bit Commitment

Public parameters: $\Phi = \left[0, 2^k\right)$, C and C_i

Prover **Verifier**

$x \in \Phi$, $x = \prod_{i=0}^{k-1} x_i 2^i$

$C = Com(x),\ C_i = Com(x_i)$

$$\xrightarrow[OR-Proof\ \sim 2\ Schnorr\ proofs]{PK\{(x_i,\ \forall i)\ :\ C_i = Com(x_i)\ \wedge\ x_i \in \{0,1\}\}}$$

Folklore Bit Commitment

Schnorr proof (the typical Σ-protocol)

Prover		**Verifier**
$x = \log_g h$		h
$d = g^u, \ u \in_R \mathbb{Z}_p$	$\xrightarrow{\quad d \quad}$	
	$\xleftarrow{\quad c \quad}$	$c \in_R \mathbb{Z}_p$
$r = u + cx$	$\xrightarrow{\quad r \quad}$	$g^r \stackrel{?}{=} dh^c$

Folklore Bit Commitment

Folklore Bit Commitment

Public parameters: $\Phi = \left[0, 2^k\right)$, $C = Com(x)$ and $C_i = Com(x_i)$

Prover **Verifier**

$x \in \Phi$, $x = \prod_{i=0}^{k-1} x_i 2^i$

$$\xrightarrow[OR-Proof\ \sim 2\ Schnorr\ proofs]{PK\{(x_i,\ \forall i)\ :\ C_i = Com(x_i)\ \wedge\ x_i \in \{0,1\}\}}$$

Properties

- Large Complexity: $O(k)$
- 2x loss of efficiency for arbitrary upperbound: $\Phi = [0, H]$.

Lipmaa, Asokan, Niemi, 2002

- Decompose $[0, H]$ as following:
  $[0, H] = \sum_{i=0}^{\log_2 H-1} G_i * [0, 1]$ with $G_i := \lfloor (H + 2^i)/2^{i+1} \rfloor$.
- Twice more efficient than folklore proof for arbitrary H.
- Easy to prove that $x_i \in [0, 1]$.
- Communication complexity: $\Theta(\log H)$.
- Did not use the language of additive combinatorics.

CCS'08

Camenisch, Chaabouni, Shelat 2008

- Write $[0, u^\ell - 1] = \sum u^i * [0, u-1]$.
- Efficient ZK proof that $C_i = Com(x_i) \wedge x_i \in [0, u-1]$ done by letting the verifier sign the values $0, \ldots, u-1$, and the prover to prove that he knows signatures on all values x_i.
- Uses specific signature scheme based on bilinear pairings.
- By selecting optimal u, the communication complexity is $\Theta(\log H / \log\log H)$.
- Missing restriction for the OR-composition.
- If $H \neq u^\ell - 1$, twice less efficient.

Contribution

Problem that we solved

- Generalize LAN'02 to the case $u > 2$.
  - LAN'02: $[0,H] = \sum_{i=0}^{\log_2 H-1} G_i * [0,1]$ with $G_i := \lfloor (H+2^i)/2^{i+1} \rfloor$.
  - CCS'08: $[0,u^\ell - 1] = \sum u^i * [0,u-1]$.
- Write $[0,H] = \sum_{i=0}^{\ell-1} G_i * [0,u-1] + [0,H']$.
  - $\ell \leqslant \log_u(H+1)$ and $H' < u-1$.
  - if $(u-1) \mid H$ then $H' = 0$.
- We provide a semi-closed form to compute G_i.

Intuition

Basic Idea

- First write: $[0, H] = [0, H_0] = G_0 * [0, u-1] + [0, H_1]$.
- Optimal G_0 is: $G_0 = \lfloor (H_0 + 1)/u \rfloor$.
- Hence $H_1 = H_0 - (u-1)G_0$.
- If $H_1 \geqslant u - 1$, then recursively set

  $G_i = \lfloor (H_i + 1)/u \rfloor$,

  $H_{i+1} = H_i - (u-1)G_i$.
- This process stops within $\ell \leqslant \log_u(H+1)$ steps.
- Hence $H' = H_\ell = H - (u-1) \cdot \sum_{i=0}^{\ell-1} G_i = H - (u-1) \cdot \lfloor H/(u-1) \rfloor$.

Theorems

New Range Proof

We can write $[0,H] = \sum_{i=0}^{\ell-1} G_i * [0,u-1] + [0,H']$, *with* $\ell \leqslant \log_u(H+1)$, G_i *given by recursive formulas, and* $H' = H - \lfloor H/(u-1) \rfloor \cdot (u-1)$.

Optimal case reached when $u \approx \log_2 H / \log_2 \log_2 H$.

Theorems

Semi-Closed Form for G_i

Let $H = \sum h_i u^i$. *Then* $G_i = \left\lfloor \frac{H}{u^{i+1}} \right\rfloor + \left\lfloor \frac{h_i + 1 + \left(\sum_{j=0}^{i-1} h_j \mod (u-1)\right)}{u} \right\rfloor$.

See the paper for a proof by induction (requires some case analysis).

LAN'02 result follows with $u = 2$.

Additional Optimization

More Details

- Recall that if $(u-1) \mid H$ then $H' = 0$.
- Instead of $x \in [0, H]$, we prove that $(u-1)x \in [0, (u-1)H]$.
- Range proof twice more efficient than CCS'08 for general H.

Conclusion

- New range proof, twice more efficient than state of the art.
- Errors in CCS'08 corrected.
- Still room for further work (journal paper in progress).

Questions?

- LAN'02: Helger Lipmaa, N. Asokan and Valtteri Niemi. Secure Vickrey Auctions without Threshold Trust. In Matt Blaze, editor, Financial Cryptography 2002, volume 2357 of Lecture Notes in Computer Science, pages 85-101, Southampton Beach, Bermuda, March 11-14, 2002. Springer-Verlag.
- CCS'08: Jan Camenisch, Rafik Chaabouni, and abhi shelat. Efficient protocols for set membership and range proofs. In Josef Pieprzyk, editor, ASIACRYPT, volume 5350 of Lecture Notes in Computer Science, pages 234-252. Springer, 2008.