Shorter Quasi-Adaptive NIZK Proofs for Linear Subspaces

Charanjit Jutla and Arnab Roy

IBM Research Fujitsu Labs

Groth Sahai NIZK based on XDH

- Groups G_1, G_2 with a bilinear map $e\colon G_1 \times G_2 \rightarrow G_T$
- CRS is 4 G_2 elements: $P, Q = P^a, R = P^b, S = P^{ab}$ or P^{ab+1}
- Proof of (g^x, f^x) in G_1 is:
  - Choose u at random
  - Commitment to witness: $Q^x P^u, S^x R^u$
  - Proof for each equation: g^u, f^u
- The commitment is hiding/binding depending on the choice of S
- Verification involves 12 pairings

Quasi-Adaptive NIZK

- CRS construction depends on the group constants
- No knowledge of trapdoor required for CRS construction
  - Such as the discrete logs of the group constants
- Zero-knowledge simulation also does not require discrete log of group constants
- Soundness proof requires discrete log of the group constants
  - Hence the group constants have to be generated 'honestly' - formally, from a known witness samplable distribution
- In most practical situations this is fine
  - Typically hard language chosen at setup by an honest party

Our Proof System – DH example

- Version based on the XDH assumption:
  - Groups G_1, G_2 with a bilinear map $e\colon\ G_1 \times G_2 \to G_T$
  - DDH assumption in G_2
  - Consider the same language in G_1 with base elements $(g, f) \in G_1^2$
  - CRS is
    - For prover, 1 G_1 element: $S = g^d f^{b^{-1}}$ for random d, b
    - For verifier, is 3 G_2 elements: g_2, g_2^{bd}, g_2^{-b}
  - Proof of (g^x, f^x) is just S^x
  - Verification: $e(g^x, g_2^{bd}). e(f^x, g_2). e(S^x, g_2^{-b}) = 0_T$

Our Proof System - General

- In general, a linear subspace language is given as:
$$L = \{\vec{x}.\boldsymbol{A} \in G_1^n \mid x \in \mathbb{Z}^t\}$$
- <u>Additive</u> group notation
- Here $\boldsymbol{A}^{t \times n}$ is the parameter of the language

- For example, our DH language is:
  - $x.[\boldsymbol{g} \;\; \boldsymbol{f}]$

- The DLIN language $(\boldsymbol{g}^x, \boldsymbol{f}^y, \boldsymbol{h}^{x+y})$ is:
  - $[x \;\; y] . \begin{bmatrix} \boldsymbol{g} & 0 & \boldsymbol{h} \\ 0 & \boldsymbol{f} & \boldsymbol{h} \end{bmatrix}$

- Think of the first t elements of a candidate l as the 'free' elements and the rest s (= n-t) elements as the dependent elements
- This amounts to assuming A as a full-ranked matrix with left $t \times t$ matrix non-singular

Our Proof System - General

- So, given $L = \{\vec{x}.\boldsymbol{A}^{t\times n} \in G_1^n \mid \vec{x}^{1\times t} \in \mathbb{Z}^t\}$
  - Generate CRS for prover: $\boldsymbol{CRS}_p = \boldsymbol{A}^{t\times n}.\begin{bmatrix} D^{t\times s} \\ b^{-1}.I^{s\times s} \end{bmatrix}$
  - Generate CRS for verifier: $\boldsymbol{CRS}_v = \begin{bmatrix} b.D^{t\times s} \\ I^{s\times s} \\ -b.I^{s\times s} \end{bmatrix}.\mathbf{g}_2$
- Now, given a candidate $\vec{l}$ with witness $\vec{x}$
  - The proof is:

$$\vec{p} = \vec{x}.\boldsymbol{CRS}_p$$

  - Verification is:

$$e([\vec{l}\;\vec{p}], \boldsymbol{CRS}_v) = \mathbf{0}_T^{n+s}$$

Comparison

- n : the number of equations
- t : the number of witnesses

		Groth Sahai	Jutla R.
XDH	Proof Size	n+2t	n-t
	CRS Size	4	2t(n-t)+2
	#Pairings	2n(t+2)	(n-t)(t+2)
DLIN	Proof Size	2n+3t	2n-2t
	CRS Size	9	4t(n-t)+3
	#Pairings	3n(t+3)	2(n-t)(t+2)

Conceptual Comparison

- n : the number of equations
- t : the number of witnesses

Groth Sahai	**Jutla R.**
CRS independent of language constants	CRS dependent on the language constants
Each witness is taken to a higher dimensional space: • 2 for XDH, 3 for DLIN	No special treatment of witnesses. The first t elements of the candidate are themselves treated as witnesses.
Each of the n equations is checked by pairing with the commitments • Along 2 dims for XDH, 3 for DLIN	Only the remaining n-t 'dependent' elements are checked by pairing • Along 1 dim for XDH, 2 for DLIN
With hiding CRS: Perfect ZK, Comp Sound With binding CRS: Comp ZK, Perfect Sound	There is no analogous hiding/binding CRS concept. Perfect ZK, Comp Sound
Since the properties are based on the indistinguishability of the two types of CRSes, the system is fundamentally based on a decision problem.	Soundness can be based on the following Computational problem: $Given\ g_2, g_2^b\ in\ G_2, find\ f, h\ in\ G_1$ $such\ that\ h = f^b \neq 0_1$

Results

- Extension for tag-based systems
  - Non-trivial since tag may be decided by adversary at runtime
  - Allows us to do Cramer-Shoup style smooth projective hashes
- Single-round password-based key exchanges, based on SXDH, with 7 group elements in each transmission
  - Previously 10 [JR12], 22 [KV11]
  - In this Crypto, 6 [Benhamouda et al] based on DDH
- Signature based on SXDH: 5 group elements
- Shortest (by ciphertext size) known IBE under SXDH: 4 group elements+1tag
  - Recently 5 group elements [CLLWW12]
- CCA-2 secure, publicly verifiable IBE under SXDH: 6 group elements + 1tag