Documentation

automatically produced by the CACE WP3 ZK-PoK Compiler

Tuesday, December 06, 2011 at 23:41:22

Note: For optimization reasons, the specified `ProofGoal` was (potentially) rewritten to `P_1`.

1 Declarations and Inputs

1.1 Common Declarations

$p \quad \in \quad \mathbb{P}_{1024}$
$q \quad \in \quad \mathbb{P}_{160}$
$k_{sec} = 80 \quad \in \quad \mathbb{Z}$
$y, g \quad \in \quad \mathbb{Z}_p^*$

1.2 Private Declarations – Prover

1.2.1 Prover's Inputs

$x \quad \in \quad \mathbb{Z}_q$

1.2.2 Global Variables

$\mathbf{s_1}, \mathbf{r_1} \quad \in \quad \mathbb{Z}_q$

1.3 Private Declarations – Verifier

1.3.1 Global Variables

$\mathbf{t_1} \quad \in \quad \mathbb{Z}_p^*$

$\mathbf{c} \quad \in \quad \{0,1\}^{80}$

2 Protocol Rounds

2.1 Prover – Round1

$\mathbf{r_1} \in_R \mathbb{Z}_q$

$\mathbf{t_1} := g^{\mathbf{r_1}}$

$$\xrightarrow{\qquad\qquad\mathbf{t_1};\qquad\qquad}$$

2.2 Verifier – Round1

$\mathbf{c} \in_R \{0,1\}^{80}$

$$\xleftarrow{\qquad\qquad\mathbf{c};\qquad\qquad}$$

2.3 Prover – Round2

$\mathbf{s_1} := \mathbf{r_1} + x \cdot \mathbf{c}$

$$\xrightarrow{\quad\quad\quad\mathbf{s_1};\quad\quad\quad}$$

2.4 Verifier – Round2

$$\mathbf{s_1} \overset{?}{\in} \mathbb{Z}_q$$
$$\mathbf{t_1} \cdot y^{\mathbf{c}} \overset{?}{=} g^{\mathbf{s_1}}$$