ElGamal Proof of Knowledge of Plaintext

SAS

January 17 2019

1 Introduction

The Zero Knowledge Argument for plaintext knowledge presented in Figure 1 of [1], instantiated to ElGamal.

1.1 NIZK Proof for Plaintext Knowledge

Common input: Ciphertext $C = (c_1, c_2)$ and public key g, y.

Prover's input: Message m and randomiser r such that $C = E(m; r)$, i.e. $C = (g^r, m.y^r)$, i.e. $c_1 = g^r$ and $c_2 = m.y^r$.

1.2 Proof

Choose:

- $k_m \in \mathbb{G}$ (i.e. a random message)
- $k_r \in \mathbb{Z}_q$ (i.e. a random exponent)

Define:

- $c_{R,1} = g^{k_r}$
- $c_{R,2} = k_m.y^{k_r}$
- $c = H(c_1, c_2, c_{R,1}, c_{R,2}, \ldots)$
- $\overline{m} = m^c.k_m$
- $\overline{k} = r.c + k_r$
- $\overline{c_1} = g^{\overline{k}} = g^{r.c+k_r}$
- $\overline{c_2} = \overline{m}.y^{\overline{k}} = m^c.k_m.y^{r.c+k_r}$

Prover's output: $(c_{R,1}, c_{R,2}, \overline{c_1}, \overline{c_2})$

Verification

- $c_1^c.c_{R,1} \stackrel{?}{=} \overline{c_1}$
- $c_2^c.c_{R,2} \stackrel{?}{=} \overline{c_2}$

If these two checks succeed then the NIZKP of plaintext knowledge has been verified.

References

[1] Jens Groth. Non-interactive zero-knowledge arguments for voting. In *Applied Cryptography and Network Security, Third International Conference, ACNS 2005, New York, NY, USA, June 7-10, 2005, Proceedings*, pages 467–482, 2005.