

# Non-interactive zero-knowledge proof of SHE

2018/Mar/20

## 1 Notations

$G_1 = \langle g_1 \rangle$  ; DLP is hard,  
 $G_2 = \langle g_2 \rangle$  ; DLP is hard,  
 $sk = (s_1, s_2)$  ; secret keys,  
 $pk = (h_1, h_2)$  ; public keys where  $h_1 = g_1^{s_1}$ ,  $h_2 = g_2^{s_2}$ .  
 $Enc(m) = (c_1, c_2, c_3, c_4) = (g_1^\rho, g_1^m h_1^\rho, g_2^\sigma, g_2^m h_2^\sigma)$  where  $\rho, \sigma \leftarrow \mathbb{Z}_p$ .

## 2 Equality of DLs

### 2.1 Prove

$r_\rho, r_\sigma, r_m \leftarrow \mathbb{Z}_p$ ,  
 $(R_1, R_2, R_3, R_4) = (g_1^{r_\rho}, g_1^{r_m} h_1^{r_\rho}, g_2^{r_\sigma}, g_2^{r_m} h_2^{r_\sigma})$ ,  
 $c = H(pp, pk, c_1, c_2, c_3, c_4, R_1, R_2, R_3, R_4)$ ,  
 $(s_\rho, s_\sigma, s_m) = (r_\rho + c\rho, r_\sigma + c\sigma, r_m + cm)$ ,  
output  $(c, s_\rho, s_\sigma, s_m)$ .

### 2.2 Verify

verify  $c = H(pp, pk, c_1, c_2, c_3, c_4, R'_1, R'_2, R'_3, R'_4)$ ,  
where  $(R'_1, R'_2, R'_3, R'_4) = (g_1^{s_\rho} / c_1^c, g_1^{s_m} h_1^{s_\rho} / c_2^c, g_2^{s_\sigma} / c_3^c, g_2^{s_m} h_2^{s_\sigma} / c_4^c)$ .

### 2.3 Correctness

$$\begin{aligned} R'_1 &= g_1^{s_\rho - c\rho} = g_1^{r_\rho} = R_1, \\ R'_2 &= g_1^{s_m - cm} h_1^{s_\rho - c\rho} = g_1^{r_m} h_1^{r_\rho} = R_2, \\ R'_3 &= g_2^{s_\sigma - c\sigma} = g_2^{r_\sigma} = R_3, \\ R'_4 &= g_2^{s_m - cm} h_2^{s_\sigma - c\sigma} = g_2^{r_m} h_2^{r_\sigma} = R_4. \end{aligned}$$

### 3 $m = 0$ or $1$

#### 3.1 Prove

$$\begin{aligned}
d_{1-m}, s_{\rho, 1-m} &\leftarrow \mathbb{Z}_p, \\
R_{1, 1-m} &= g_1^{s_{\rho, 1-m}} / c_1^{d_{1-m}}, \\
R_{2, 1-m} &= h_1^{s_{\rho, 1-m}} / (c_2 / g_1^{1-m})^{d_{1-m}}, \\
r_{\rho, m}, r_{\rho}, r_{\sigma}, r_m &\leftarrow \mathbb{Z}_p, \\
R_{1, m} &= g_1^{r_{\rho, m}}, \\
R_{2, m} &= h_1^{r_{\rho, m}}, \\
c &= H(pp, pk, c_1, c_2, R_{1,0}, R_{2,0}, R_{1,1}, R_{2,1}), \\
d_m &= c - d_{1-m}, \\
s_{\rho, m} &= r_{\rho, m} + d_m \rho, \\
\text{output } &(d_0, d_1, s_{\rho, 0}, s_{\rho, 1}).
\end{aligned}$$

#### 3.2 Verify

$$\begin{aligned}
R'_{1, i} &= g_1^{s_{\rho, i}} / c_1^{d_i}, \text{ for } i = 0, 1, \\
R'_{2, 0} &= h_1^{s_{\rho, 0}} / c_2^{d_0}, \\
R'_{2, 1} &= h_1^{s_{\rho, 1}} / (c_2 / g_1)^{d_1}, \\
c &= H(pp, pk, c_1, c_2, R'_{1,0}, R'_{2,0}, R'_{1,1}, R'_{2,1}), \\
\text{verify } &c = d_0 + d_1.
\end{aligned}$$

## 4 $m = 0$ or $1$ and Equality of DLs

### 4.1 Prove

$$\begin{aligned}
d_{1-m}, s_{\rho, 1-m} &\leftarrow \mathbb{Z}_p, \\
R_{1, 1-m} &= g_1^{s_{\rho, 1-m}} / c_1^{d_{1-m}}, \\
R_{2, 1-m} &= h_1^{s_{\rho, 1-m}} / (c_2 / g_1^{1-m})^{d_{1-m}}, \\
r_{\rho, m}, r_{\rho}, r_{\sigma}, r_m &\leftarrow \mathbb{Z}_p, \\
R_{1, m} &= g_1^{r_{\rho, m}}, \\
R_{2, m} &= h_1^{r_{\rho, m}}, \\
R_3 &= g_1^{r_{\rho}}, \\
R_4 &= g_1^{r_m} h_1^{r_{\rho}}, \\
R_5 &= g_2^{r_{\sigma}}, \\
R_6 &= g_2^{r_m} h_2^{r_{\sigma}}, \\
c &= H(pp, pk, c_1, c_2, R_{1,0}, R_{2,0}, R_{1,1}, R_{2,1}, R_3, \dots, R_6), \\
d_m &= c - d_{1-m}, \\
s_{\rho, m} &= r_{\rho, m} + d_m \rho, \\
s_{\rho} &= r_{\rho} + c \rho, \\
s_{\sigma} &= r_{\sigma} + c \sigma, \\
s_m &= r_m + c m, \\
\text{output } &(d_0, d_1, s_{\rho, 0}, s_{\rho, 1}, s_{\sigma}, s_{\rho}, s_m).
\end{aligned}$$

### 4.2 Verify

$$\begin{aligned}
R'_{1, i} &= g_1^{s_{\rho, i}} / c_1^{d_i}, \text{ for } i = 0, 1, \\
R'_{2, 0} &= h_1^{s_{\rho, 0}} / c_2^{d_0}, \\
R'_{2, 1} &= h_1^{s_{\rho, 1}} / (c_2 / g_1)^{d_1}, \\
R'_3 &= g_1^{s_{\rho}} / c_1^c, \\
R'_4 &= g_1^{s_m} h_1^{s_{\rho}} / c_2^c, \\
R'_5 &= g_2^{s_{\sigma}} / c_3^c, \\
R'_6 &= g_2^{s_m} h_2^{s_{\sigma}} / c_4^c, \\
\text{where } c &= d_0 + d_1, \\
\text{verify } c &= H(pp, pk, c_1, c_2, R_{1,0}, R_{2,0}, R_{1,1}, R_{2,1}, R'_3, \dots, R'_6).
\end{aligned}$$

$$5 \quad m \in M := \{ m_1, \dots, m_n \}$$

### 5.1 Notations

$P$  : generator  
 $x$  : secret key  
 $Q := xP$  : public key  
 $\text{Enc}(m, r) := (mP + rQ, rP)$ ; ciphertext of  $m$

Properties:

$$\text{Enc}(m_1, r_1) + \text{Enc}(m_2, r_2) = \text{Enc}(m_1 + m_2, r_1 + r_2).$$

### 5.2 Prove

Let  $C := \text{Enc}(m, r)$  and  $m = m_{i'}$ .  
 Select  $\{ a_i \}_{i \neq i'}$  and  $\{ t_i \}$  randomly.

$$\begin{aligned}
 R_i &:= \text{Enc}(a_i(m - m_i), t_i), \\
 h &:= \text{Hash}(P, Q, C, \{ R_i \}), \\
 a_{i'} &:= h - \sum_{i \neq i'} a_i, \\
 b_i &:= t_i - a_i r.
 \end{aligned}$$

Output a proof  $\pi := \{ a_i, b_i \}$ .

### 5.3 Verify

For given  $P, Q, C, \pi := \{ a_i, b_i \}, M$ ,

$$\begin{aligned}
 R_i &:= a_i(C - \text{Enc}(m_i, 0)) + \text{Enc}(0, b_i), \\
 h &:= \text{Hash}(P, Q, C, \{ R_i \}), \\
 \text{Verify } h &= a_1 + \dots + a_n.
 \end{aligned}$$

Remark: If the verification is okay,

$$R_i = \text{Enc}(a_i(m - m_i), a_i r + b_i).$$

Let  $t_i := a_i r + b_i$ , then

$$\text{Hash}(P, Q, C, \{ \text{Enc}(a_i(m - m_i), t_i) \}) = a_1 + \dots + a_n.$$

If  $m \notin M$ , it is hard to find  $a_i, t_i$ .