$$\vdots$$

$\mathcal{P}^*$

$\mathcal{V}^*$

$\mathcal{V}^*$

$\mathcal{P}$

$\mathcal{V}$

$\mathcal{V}$

$\mathcal{P}$

$K \in_R \{0,1\}^k$

E_K

K

D_K

$E_K, D_K : \{0,1\}^k \to \{0,1\}^k$

$c \in_R \{0,1\}^k$

$r =$

$E_K(c)$

$D_K(r) =$

c

$K \in_R \{0,1\}^k$

$H :$

$\{0,1\}^* \to$

$\{0,1\}^k$

$c \in_R \{0,1\}^k$

$r =$

$H(K,c)$

$r =$

$H(K,c)$

pk

sk

E_{pk}

pk

D_{sk}

sk

$M \in_R \{0,1\}^k$

$c =$

$E_{pk}(M)$

$r =$

$D_{sk}(c)$

$r =$

M

pk

sk

S_{sk}

sk

V_{pk}

pk

$c \in_R \{0,1\}^k$

$r =$

$S_{sk}(c)$

$V_{pk}(c,r)$

r

c

pk

$\langle g \rangle$

n

$x \in_R Z_n$

$h_x =$

g^x

h

k

k

a

u

r

$x =$

log_g^h

x

a

$c =$

0

$c =$

1

$c =$

0

$a =$

g^u

$r =$

u

$c =$

1

$a =$

g^u/h

$r =$

u

$g^r =$

ah

$x =$

0

$c =$

1

$a =$

0

$c =$

1

r_0

r_1

$c =$

0

$c =$

1

r_0

r_1

$g^{r_0} = a, g^{r_1} = ah$