$commit: \{0,1\}^k \times \{0,1\}^* \rightarrow \{0,1\}^*$

k
$x \in$
$\{0,1\}^*$
$C =$
$commit(u,x)$
x
$u \in_R \{0,1\}^k$
x
C
C
x
u
x
C
x.
u
x
$C =$
$commit(u,x)$
x
C
$commit(u,x)$
C
$x \in$
$\{0,1\}$.
C
x.
x
C.
ε
$u, u' \in$
$\{0,1\}^k$
$commit(u,0) =$
$commit(u',1)$
)
(
$commit(u,0)$
$commit(u,1)$
$u \in_R \{0,1\}^k$
H
$commit_0(u,x) = H(u,x)$

$x \in$
$\{0,1\}$
$u \in$
$\{0,1\}^k$
H
u
x
u'
$1-$
x
$H(u,x) = H(u', 1-x)$

x
u
$1/2$
n
$1/2^n$
$p =$
$\ell_A^{e_A} \ell_B^{e_B}$.
$f \pm$
1
ℓ_A
ℓ_B
$\ell_A^{e_A}$
$\ell_B^{e_B}$
f
p
$\ell_A^{e_A}$
$\ell_B^{e_B}$
?
E
F_{p^2}
$(\ell_A^{e_A} \ell_B^{e_B})^2$
$E[\ell_A^{e_A}]$
$E[\ell_B^{e_B}]$
$\langle P_A, Q_A \rangle$
$\langle P_B, Q_B \rangle$
E
??
S
$\phi :$
$E \longrightarrow$
$E/\langle S \rangle$
:
ϕ
S
:
$E/\langle S \rangle$
P_B
Q_B
$\phi(P_B)$
$\phi(Q_B)$
$\phi"][d,"\psi"]E/\langle S \rangle[d,"\psi'"]$

$ch \in$
$\{0, 1\}$
$resp$
$ch =$
0
$resp =$
$(R, \phi(R))$
$ch =$
1
$resp =$
$\psi(S)$
$ch =$
0
R
$\phi(R)$
$\ell_B^{e_B}$
$E \to$
E_1
$E/\langle S\rangle \to$
E_2
$ch =$
1
$\psi(S)$
$\ell_A^{e_A}$
$E_1 \to$
E_2

$$\frac{(E/\langle S\rangle)}{\langle\phi(R)\rangle} = \frac{E}{\langle R, S\rangle} = \frac{(E/\langle R\rangle)}{\langle\psi(S)\rangle}$$

$\phi"][d, "\psi"]E/\langle S\rangle[d, "\psi'"]$
$\langle R\rangle[r, dashrightarrow, "\phi'"]E/\langle R, S\rangle$
$\phi"][d, dashrightarrow, "\psi"]E/\langle S\rangle[d, dashrightarrow, "\psi'"]$
$\langle R\rangle[r, "\phi'"]E/\langle R, S\rangle$
ϕ
λ
p
6λ
λ
λ
S
R
??
$E/\langle S\rangle$
ψ
ψ'
ϕ'
S
S
$ch =$
0
ψ
ϕ'
$ch =$
1
ϕ'
$\vdots$
$\mathcal{P}$
$\mathcal{V}^*$
$\mathcal{V}^*$
$\mathcal{P}$
$\mathcal{V}$
$\mathcal{V}$
$\mathcal{P}$
$K \in_R \{0, 1\}^k$
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
$M \in_R \{0, 1\}^k$
$c =$
$E_{pk}(M)$
$r =$
$D_{sk}(c)$