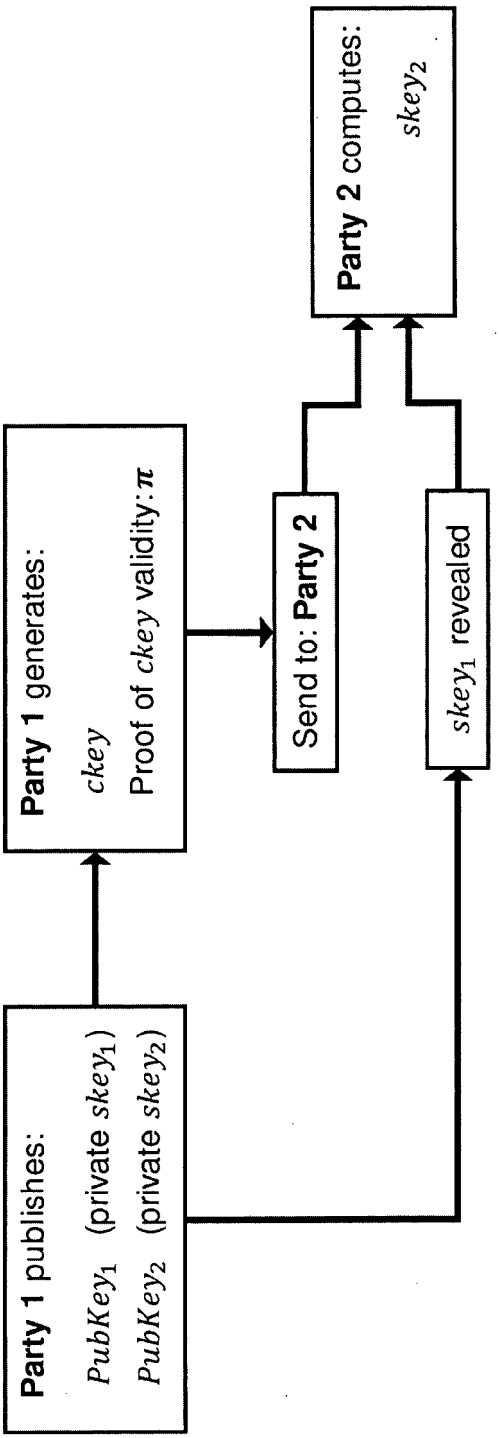

Party 1 publishes:
$PubKey_1$ (private $skey_1$)
$PubKey_2$ (private $skey_2$)
Party 1 generates:
$ckey$
Proof of $ckey$ validity: π
Send to: Party 2
$skey_1$ revealed
Party 2 computes:
$skey_2$

Fig. 1

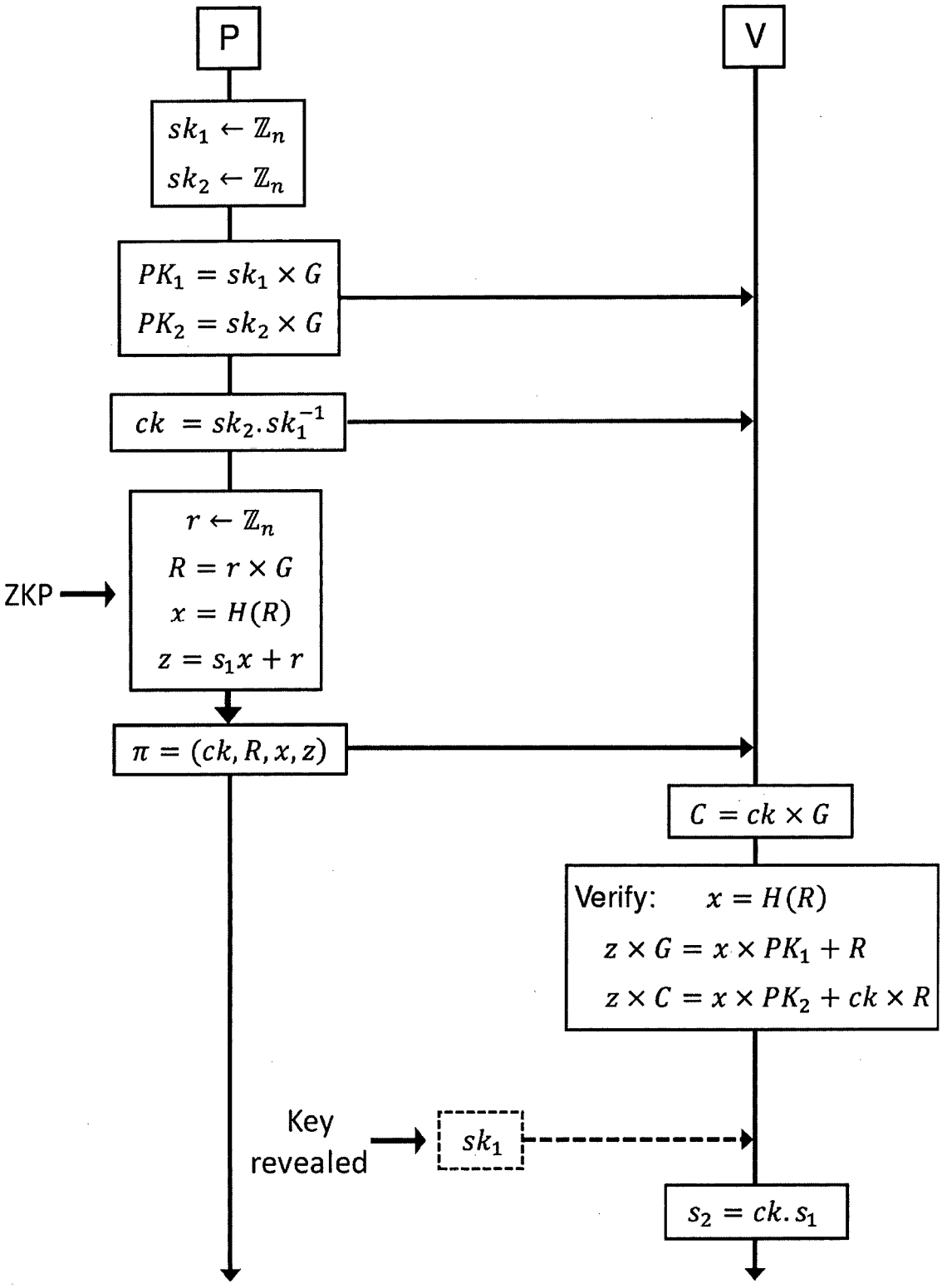

P
V
$sk_1 \leftarrow \mathbb{Z}_n$
$sk_2 \leftarrow \mathbb{Z}_n$
$PK_1 = sk_1 \times G$
$PK_2 = sk_2 \times G$
$ck = sk_2.sk_1^{-1}$
ZKP
$r \leftarrow \mathbb{Z}_n$
$R = r \times G$
$x = H(R)$
$z = s_1 x + r$
$\pi = (ck, R, x, z)$
$C = ck \times G$
Verify: $x = H(R)$
$z \times G = x \times PK_1 + R$
$z \times C = x \times PK_2 + ck \times R$
Key revealed
sk_1
$s_2 = ck.s_1$

Fig. 2

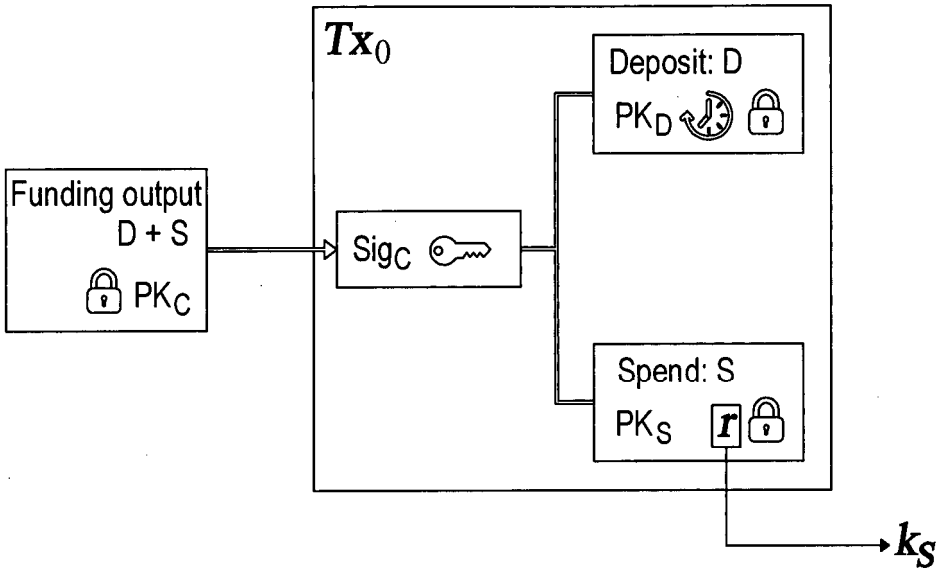


Fig. 3

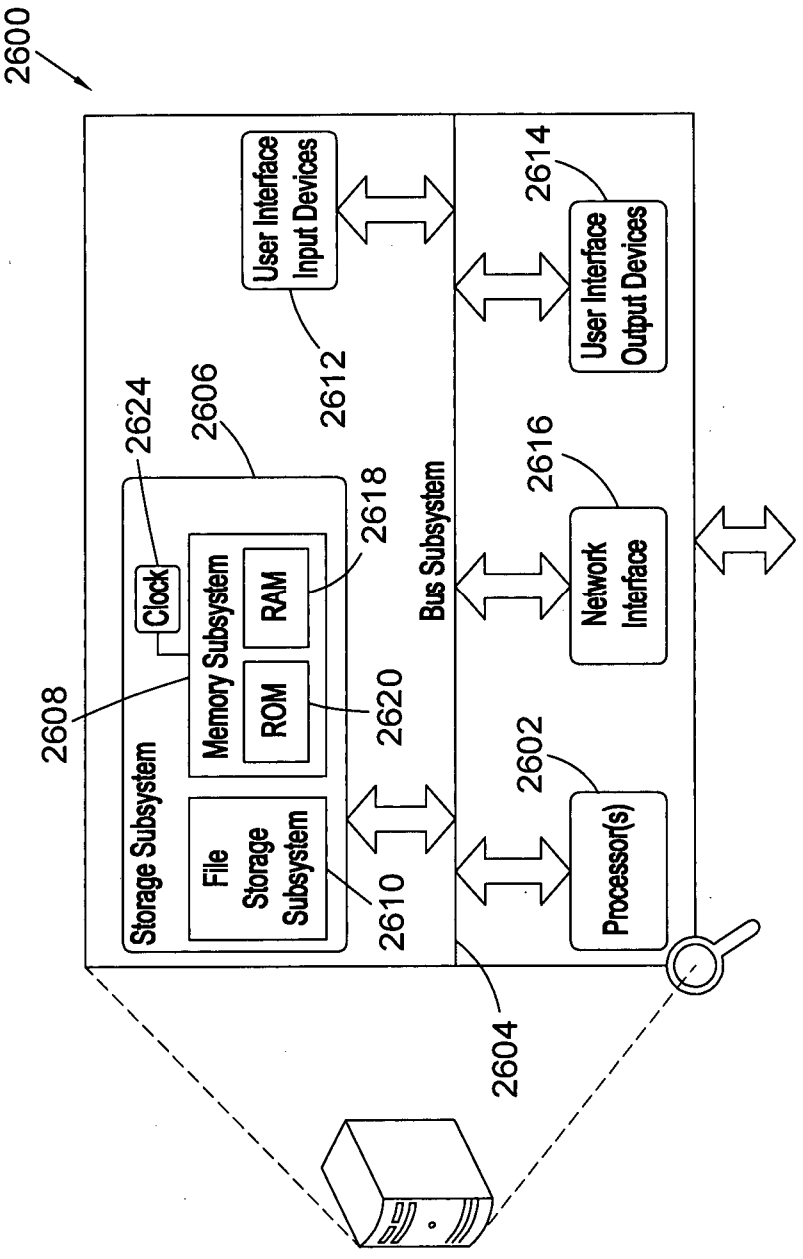

2600
User Interface Input Devices
2612
2614
User Interface Output Devices
2624
2606
2618
RAM
Clock
Memory Subsystem
2616
Network Interface
Bus Subsystem
2608
ROM
2620
Storage Subsystem
File Storage Subsystem
2610
2602
Processor(s)
2604

Fig. 4