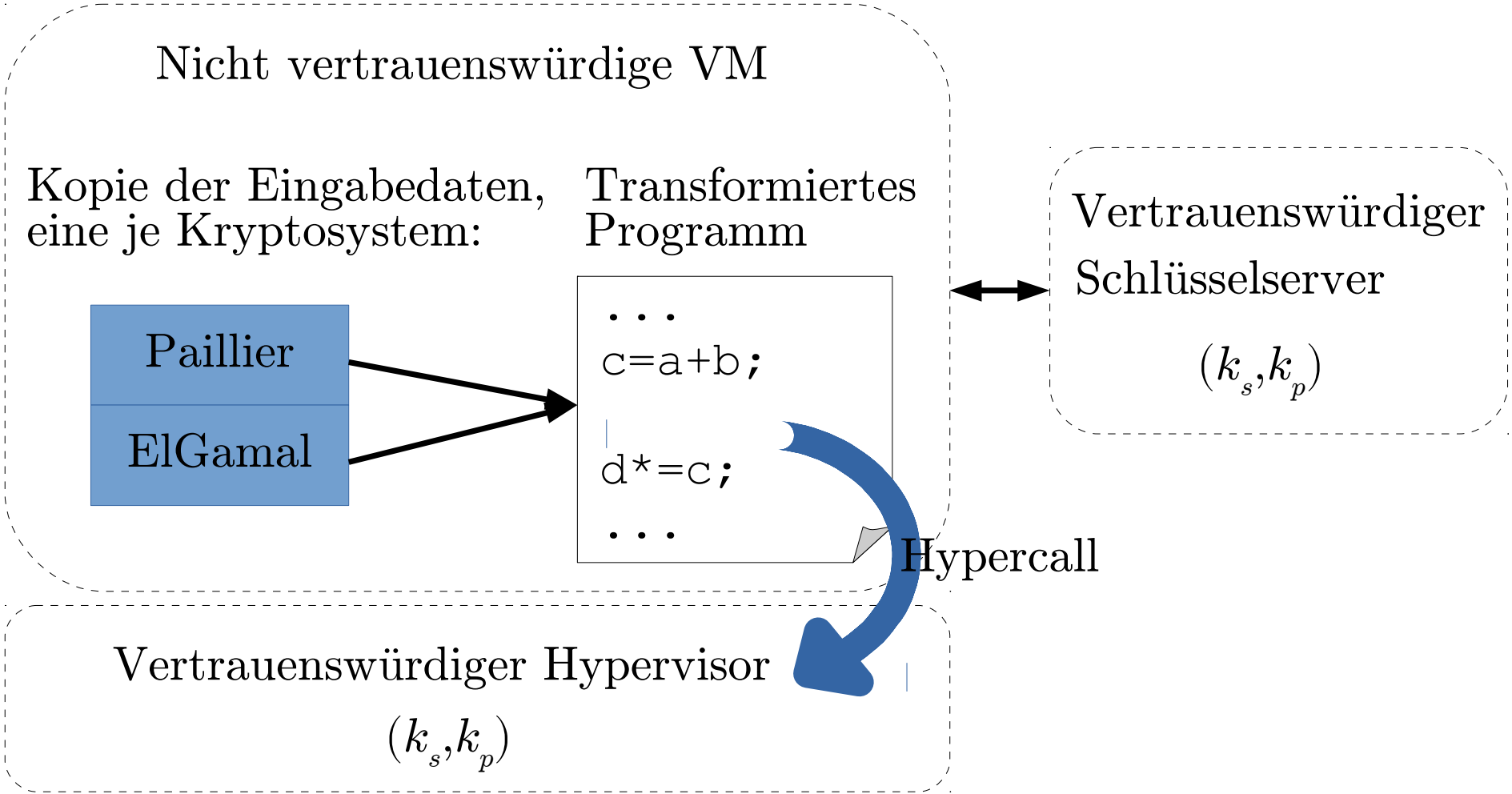
Nicht vertrauenswürdige VM
Kopie der Eingabedaten, eine je Kryptosystem:
Paillier
ElGamal
Transformiertes Programm
...
c=a+b;
d*=c;
...
Hypercall
Vertrauenswürdiger Schlüsselserver
$(k_s,k_p)$
Vertrauenswürdiger Hypervisor
$(k_s,k_p)$