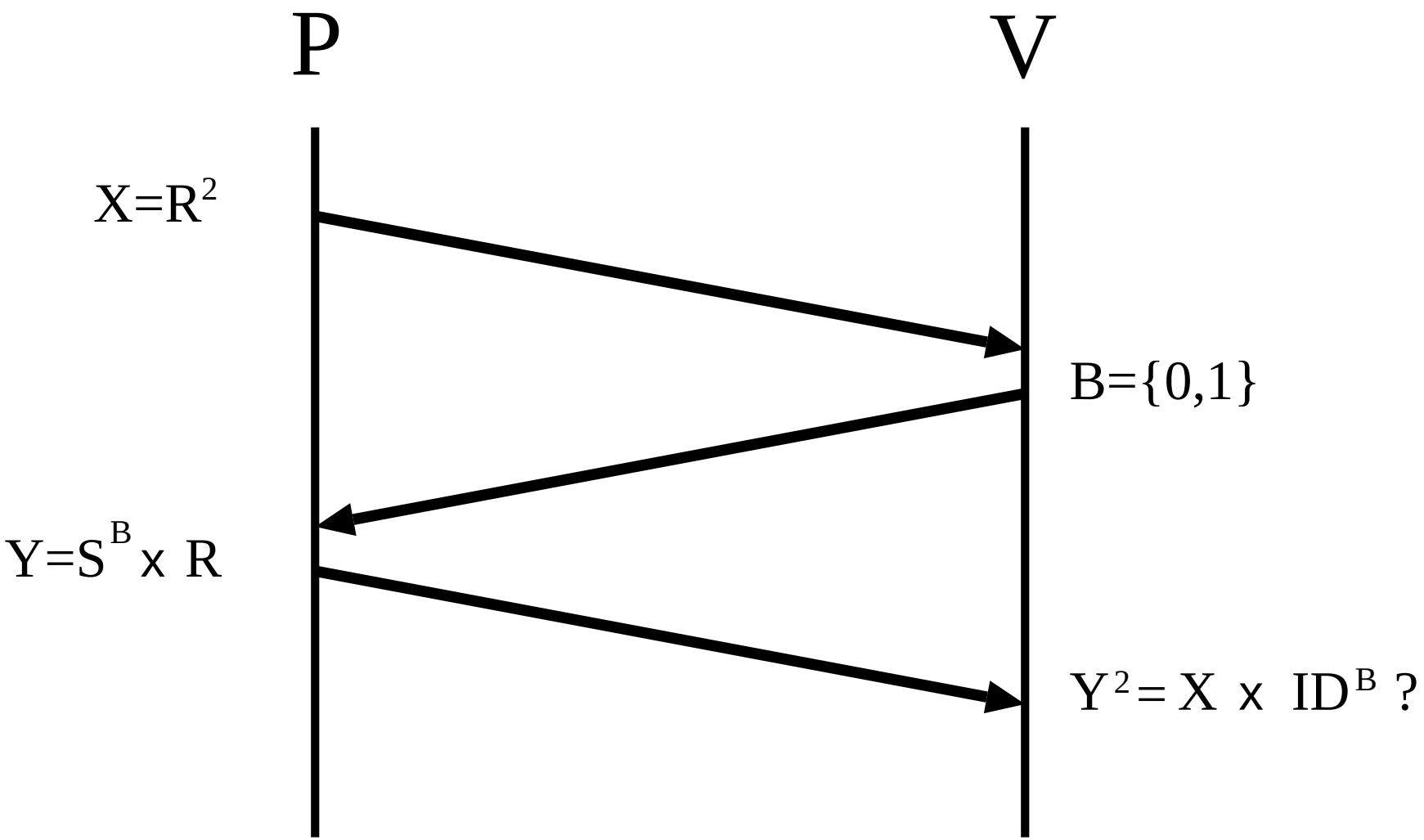
零知識相互証明(Fiat-Shamir 法)

○知識などがあることをその知識を見せずに相手に納得させる
○認証などに応用