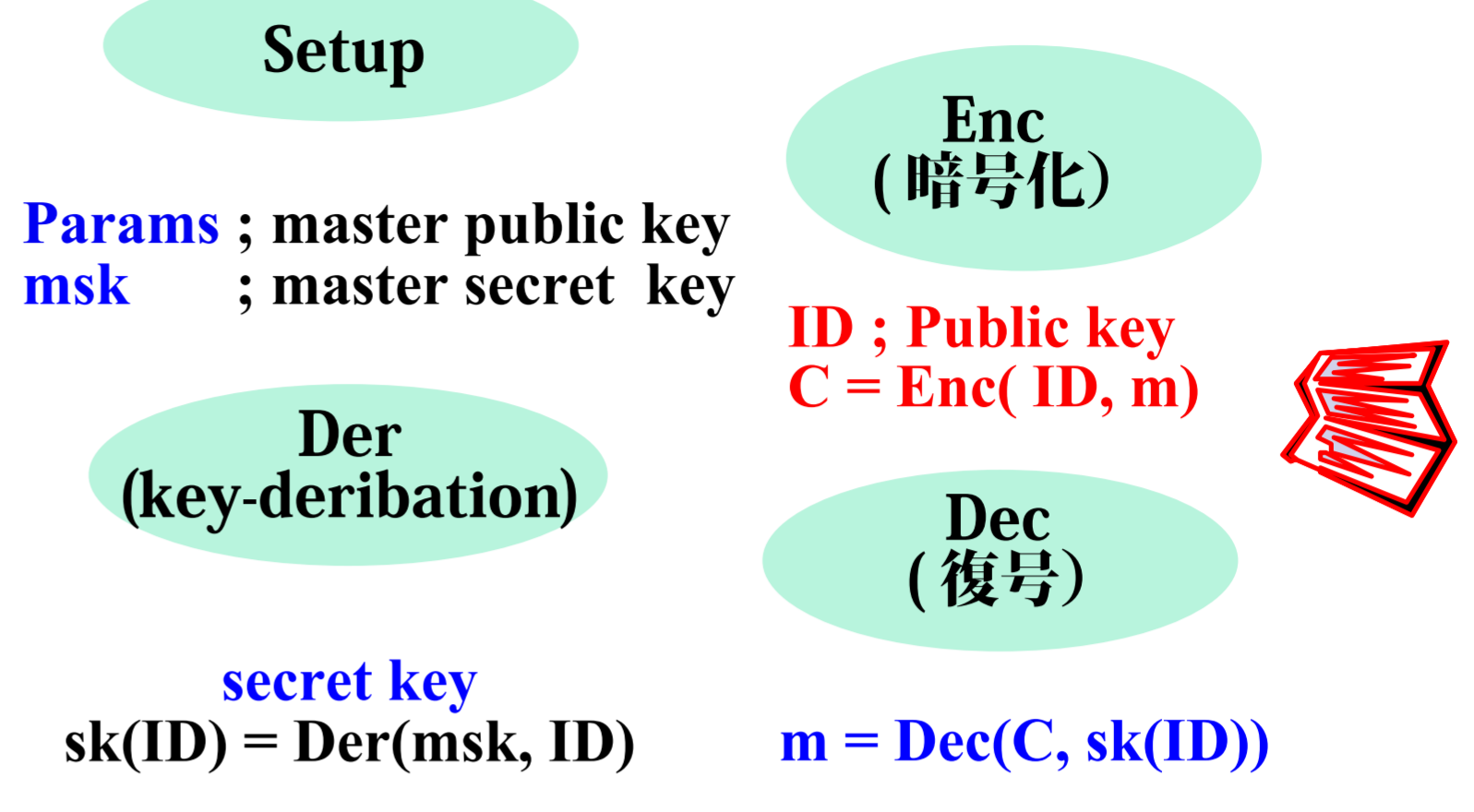
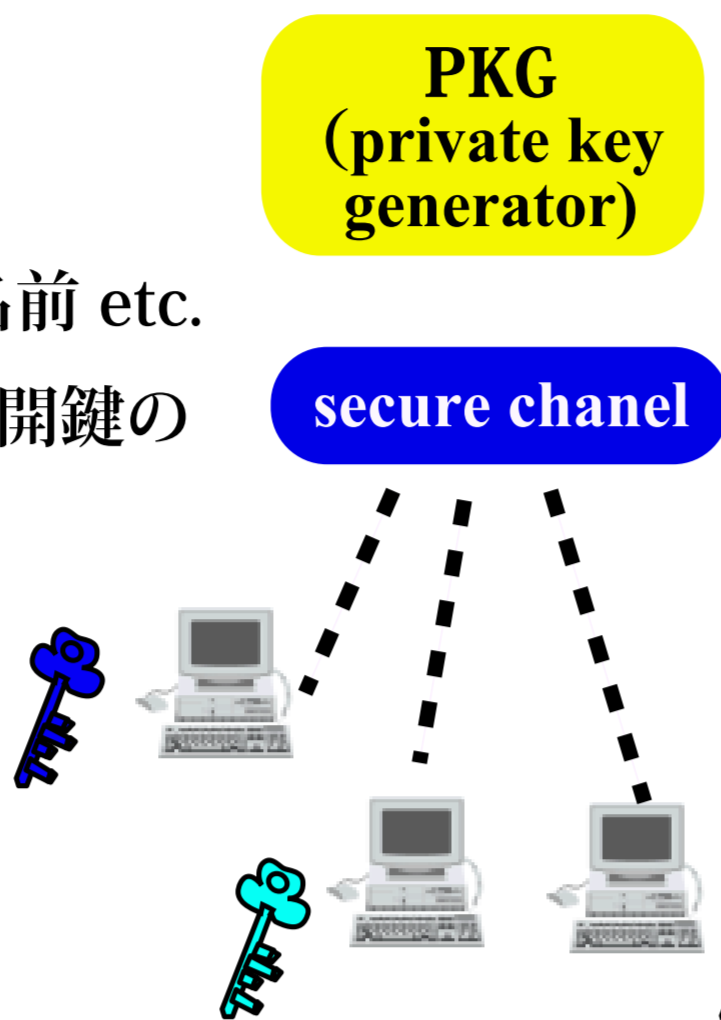
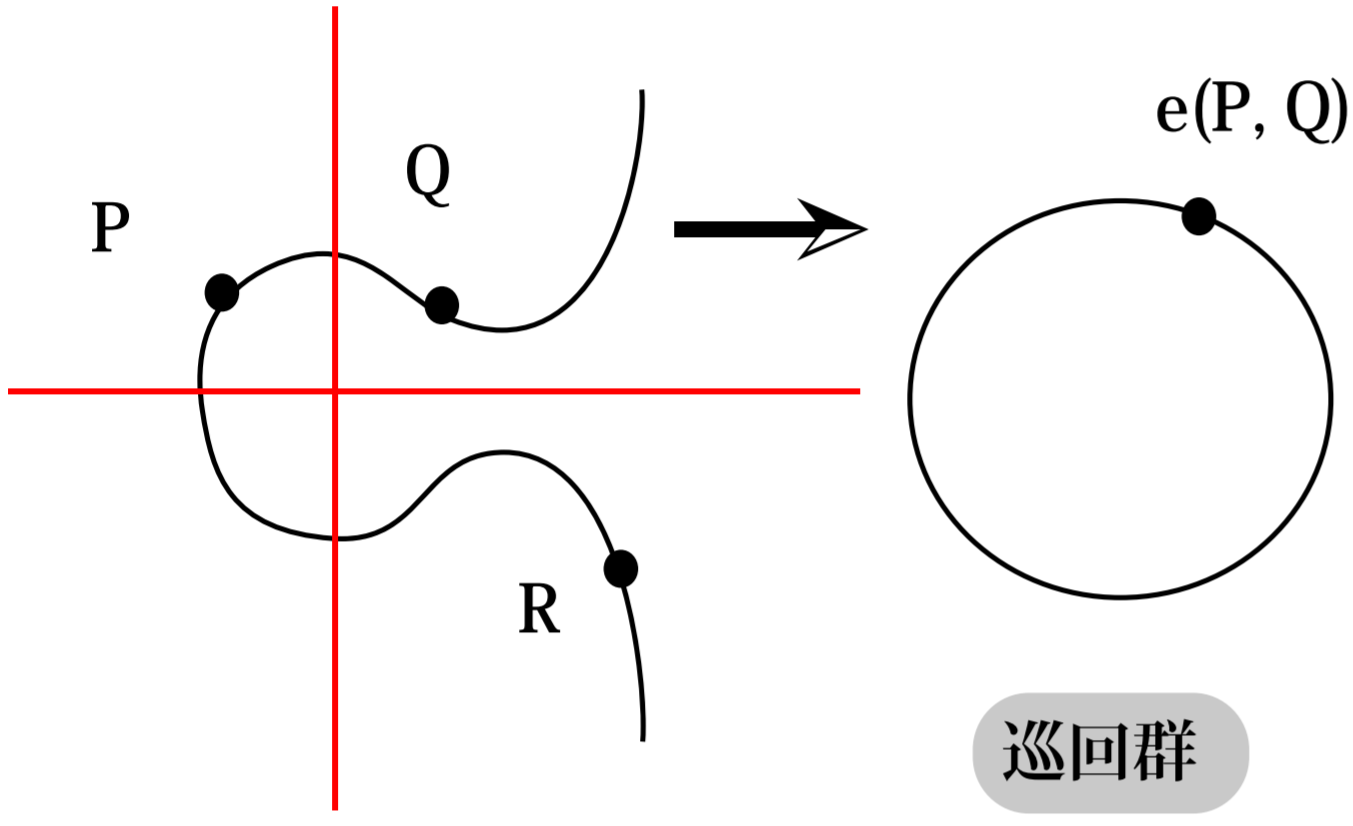


# ID ベース暗号の復号権限委譲方式によるデータ共有システム

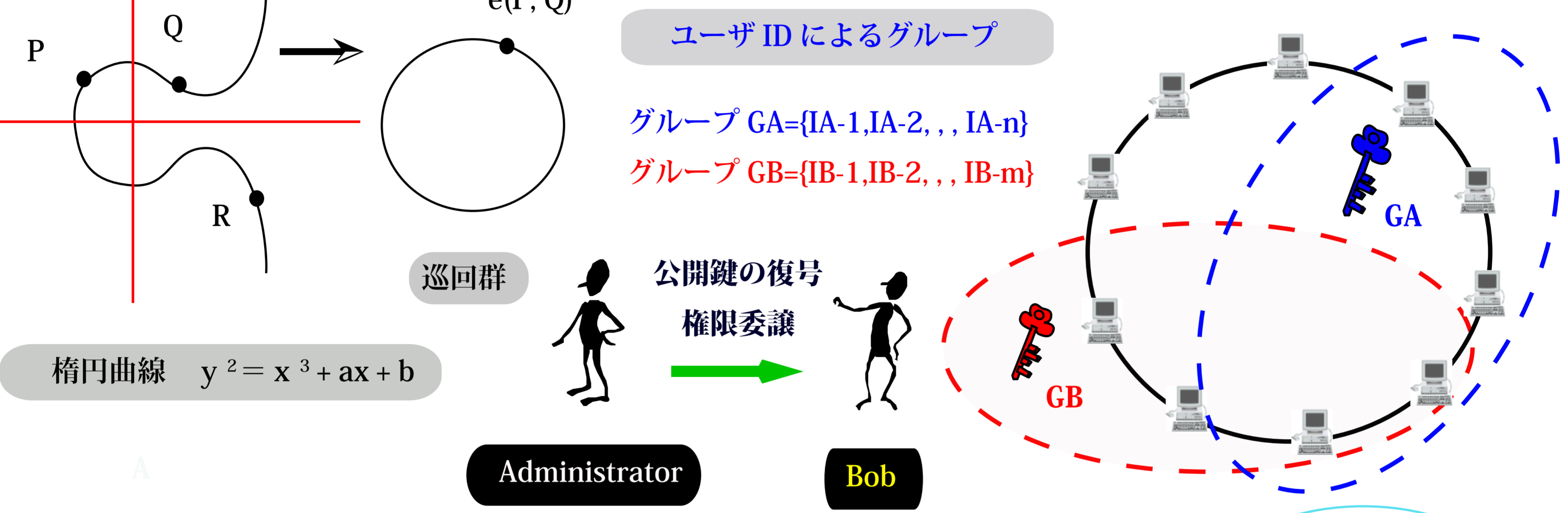
## ID ベース暗号

公開鍵 ユーザ固有の ID  
 電話番号、IP アドレス、部署名、名前 etc.  
 PKI で必要とされる認証局による公開鍵の  
 証明書が不要となる方式

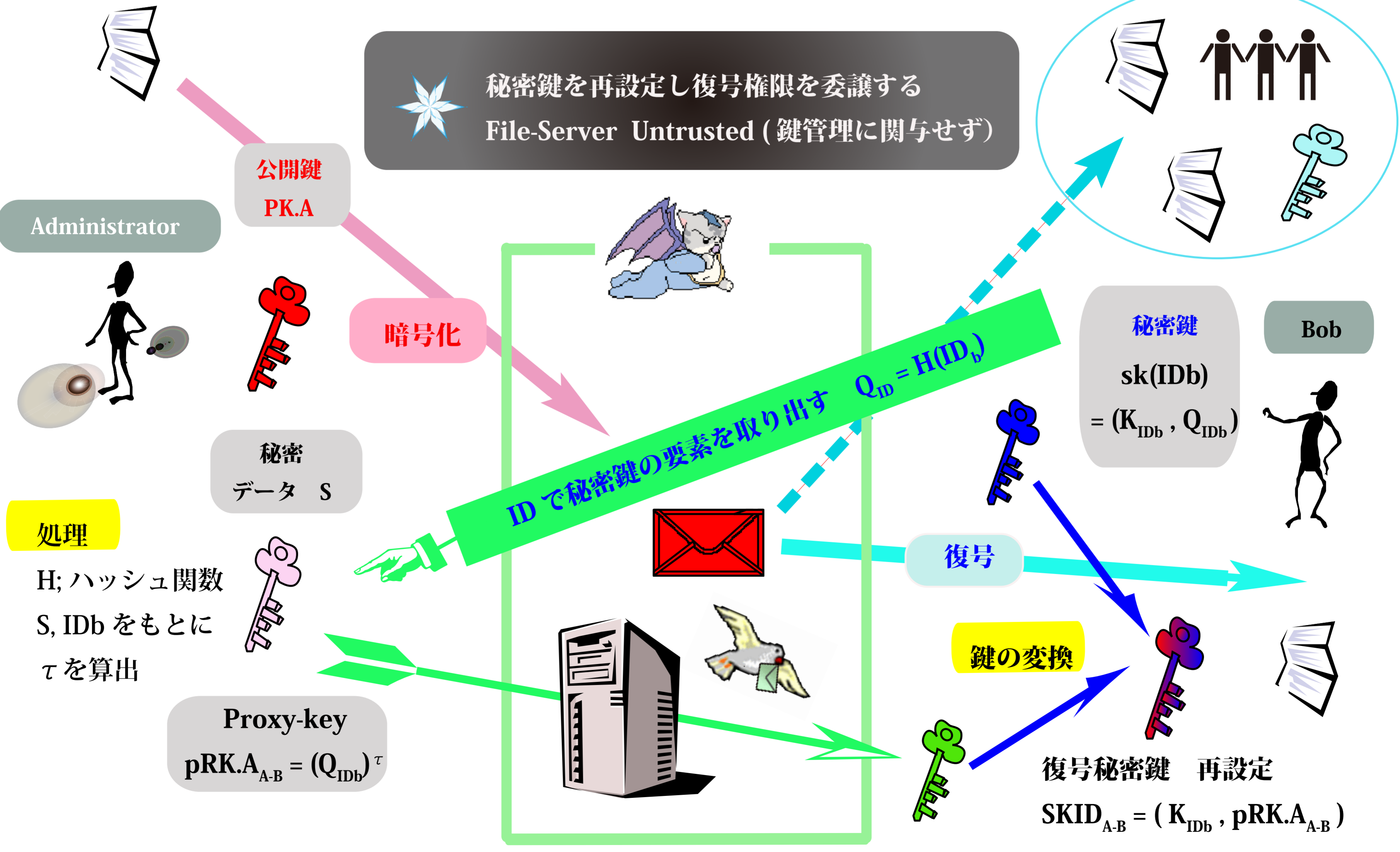
計算量的な困難性の仮定  
 加法演算  $P + Q = R$   
 pairing  $e(aP, bQ) = e(P, Q)^{ab}$



## 秘匿データの共有



秘密鍵を再設定し復号権限を委譲する  
 File-Server Untrusted (鍵管理に関与せず)



処理  
 H; ハッシュ関数  
 S, IDb をもとに  $\tau$  を算出