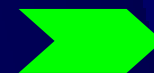


2007年度第 期
未踏ソフトウェア創造事業



IPA

IDベース暗号をもとに構成した公開鍵による
データ共有システムの開発

(利便性の高いファイル暗号の共有方式の開発)



PM ウィリアム齋藤

扇 裕和

FEK(file encryption key)の効率よい更新方式



公開鍵の共有

(1) PK.A(public-key)

Administratorが生成する
グループで暗号化データを共有する
ための公開鍵PK.A(public-key)

(2) PK.Aを復号可能な復号秘密鍵

各ユーザBob-i($1 \leq i \leq n$)

互いに相異なる秘密鍵

($i \neq j$ ならば $q_i \neq q_j$;)

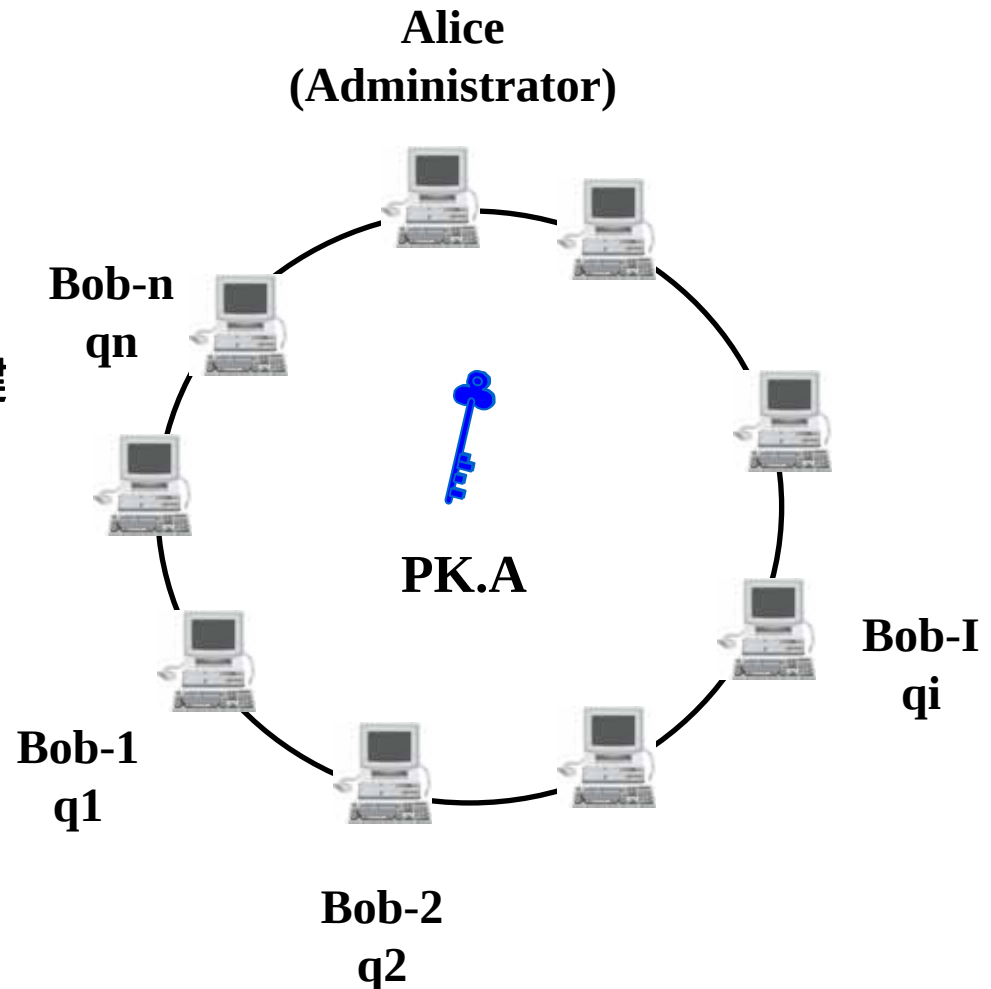
特徴

FEK(file encryption key)の暗号データ

$C = \text{Enc}(\text{PK.A}, \text{FEK})$

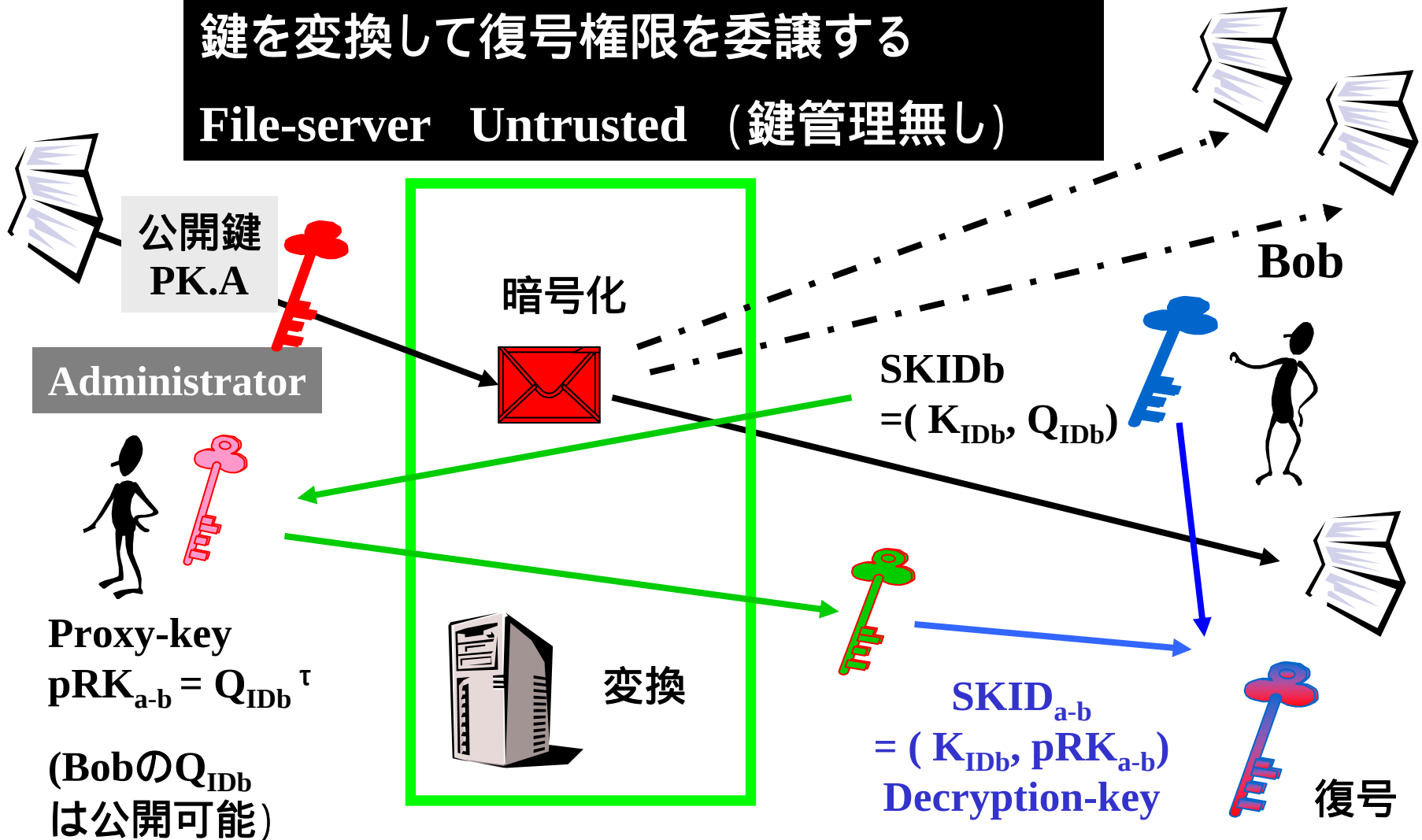
各ユーザBob-iが**1回暗号化**

グループ全員で共有できる。



IDベース暗号によるProxy-key (復号権限の委譲) ➡ *proxy*

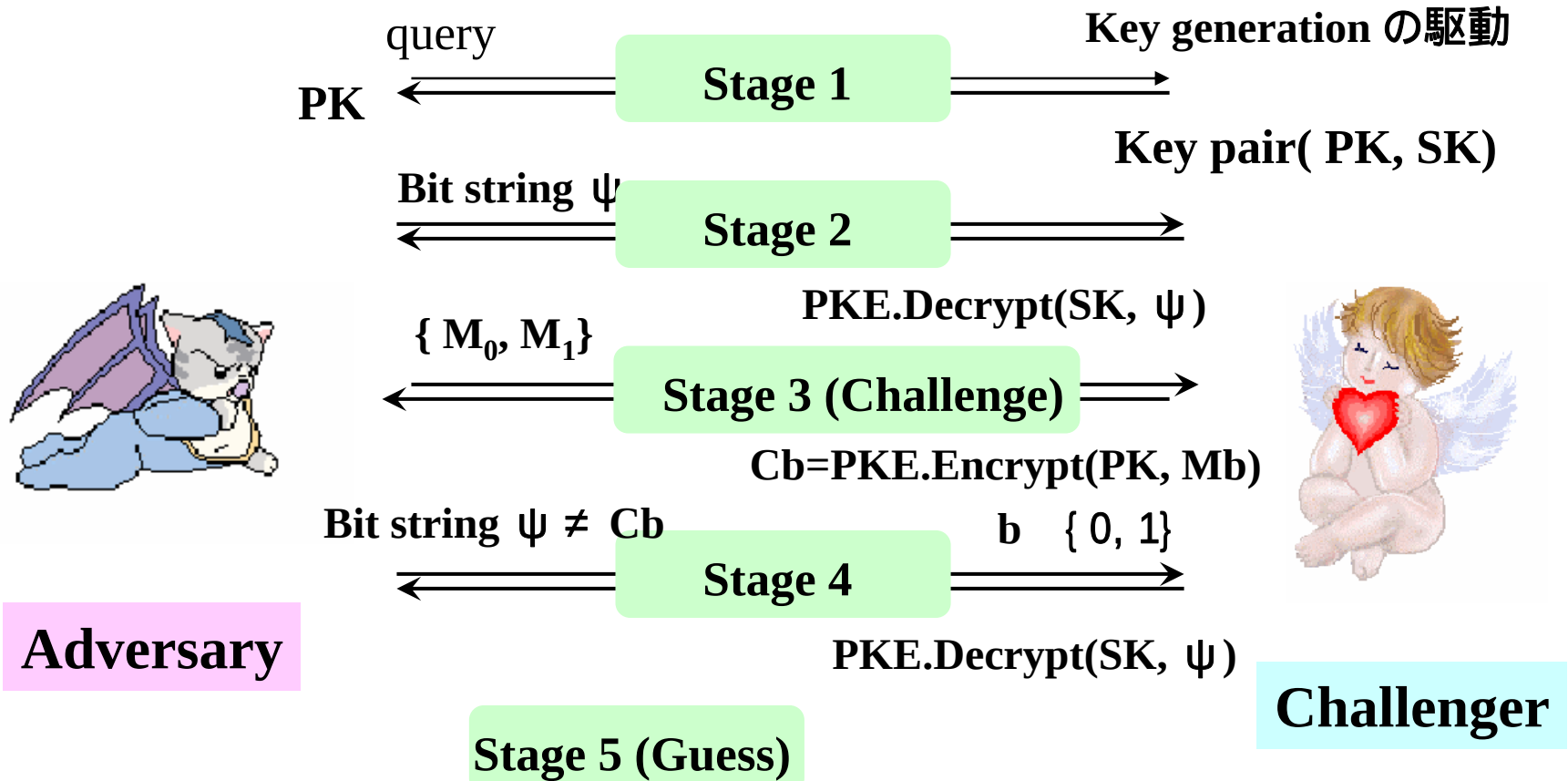
鍵を変換して復号権限を委譲する
File-server Untrusted (鍵管理無し)



IND-CCA2 (安全性)

 *proxy*

Indistinguishability adaptive chosen ciphertext attack



$$Adv^{cca}_{PKE, A} = \left| Pr[b = b^*] - \frac{1}{2} \right| \leq \varepsilon$$