2007年度第Ⅱ期
未踏ソフトウェア創造事業

IPA

IDﾍﾞ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

proxy

公開鍵の共有

(1) PK.A(public-key)

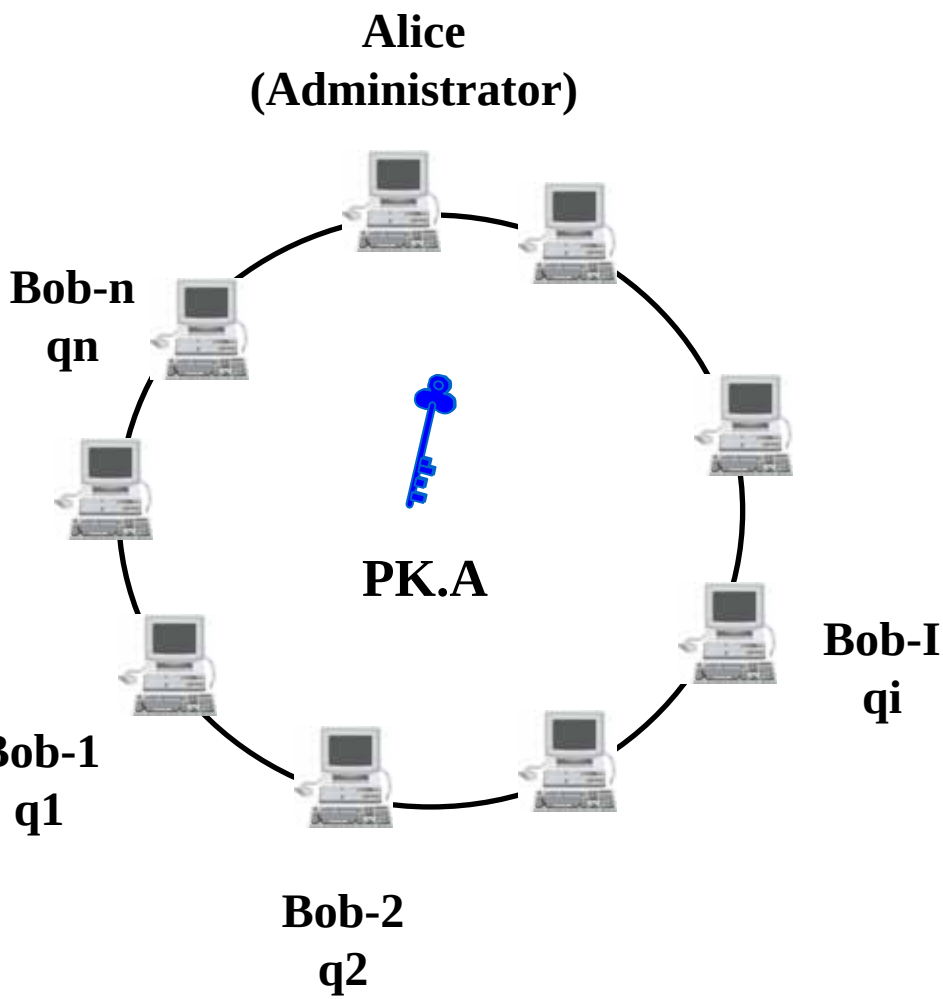
Administratorが生成する
グループで暗号化データを共有する
ための公開鍵PK.A(public-key)

(2) PK.Aを復号可能な復号秘密鍵

各ユーザBob-i(1≦i≦n)

互いに相い異なる秘密鍵

(i≠j ならば qi ≠qj;)



特徴

FEK(file encryption key)の暗号データ
C=Enc(PK.A, FEK)

各ユーザBob-iが**1回暗号化**

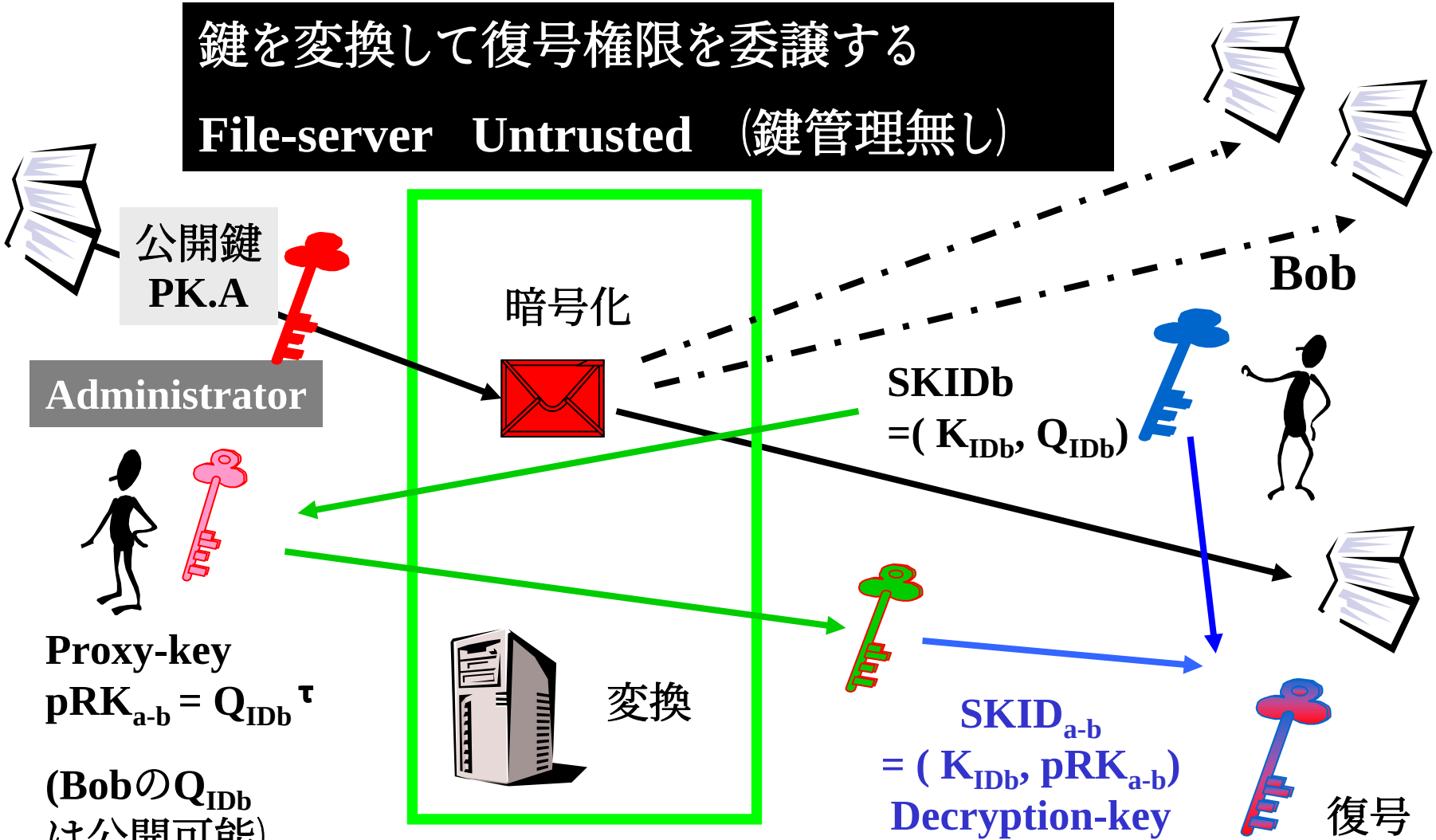
グループ全員で共有できる。

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)
Indistinguishability adaptive chosen ciphertext attack

proxy

query

PK

Key generation の駆動

Stage 1

Key pair(PK, SK)

Bit string ψ

Stage 2

PKE.Decrypt(SK, ψ)

$\{ M_0, M_1 \}$

Stage 3 (Challenge)

Cb=PKE.Encrypt(PK, Mb)

Bit string ψ ≠ Cb

b∈{ 0, 1}

Stage 4

Adversary

PKE.Decrypt(SK, ψ)

Challenger

Stage 5 (Guess)

Out put b^* ∈{ 0, 1}

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