Circular Encryption

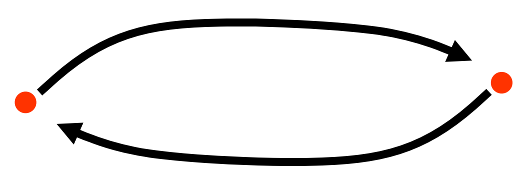
Dan Boneh Shai Halevi

Mike Hamburg Rafi Ostrovsoky

Circular encryption

- (E, D) a symmetric cipher. k_1 , k_2 two keys.
- Which of the following is “safe” to publish?

1. $c \leftarrow E_{k_1}(k_2)$ ✓
2. $c \leftarrow E_{k_1}(k_1)$ ✗
3. $c_1 \leftarrow E_{k_1}(k_2)$, $c_2 \leftarrow E_{k_2}(k_1)$ ✗



(2-circular encryption)

More generally, KDM

- Key Dependent Messages: $E_k(\ f(k)\ )$
- Why is KDM a problem? A simple example [GM'84] :

$$\hat{E}_k(m) = \begin{cases} \text{if } m=k & \text{output } c \leftarrow k \\ \text{otherwise} & \text{output } c \leftarrow E_k(m) \end{cases}$$

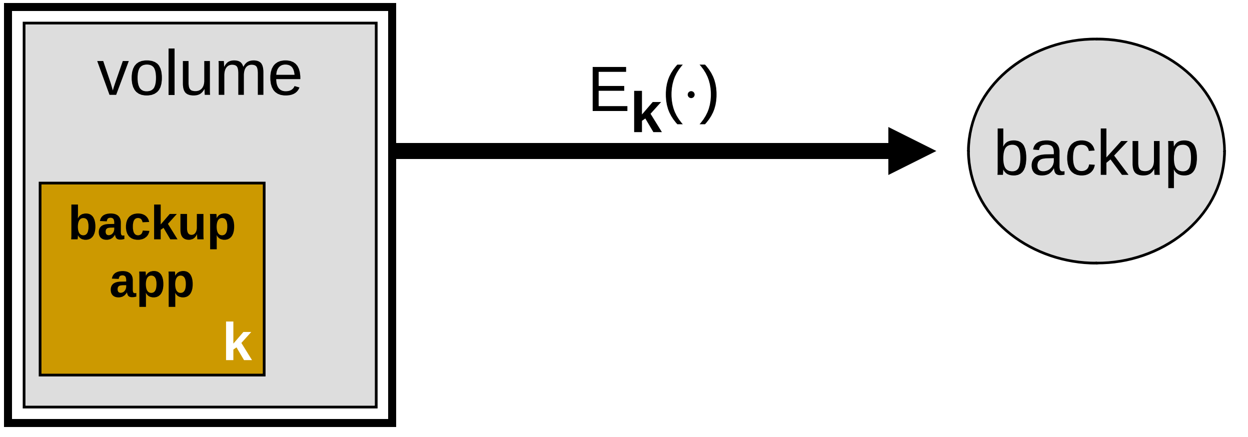
- <u>Fact</u>: E (sem) secure $\Rightarrow$ $\hat{E}$ (sem) secure

  … but publishing $\mathbf{\hat{E}_k(k)}$ breaks the system !

  $\Rightarrow$ something is wrong with our definitions of security

KDM in practice

- Encrypted backup systems:

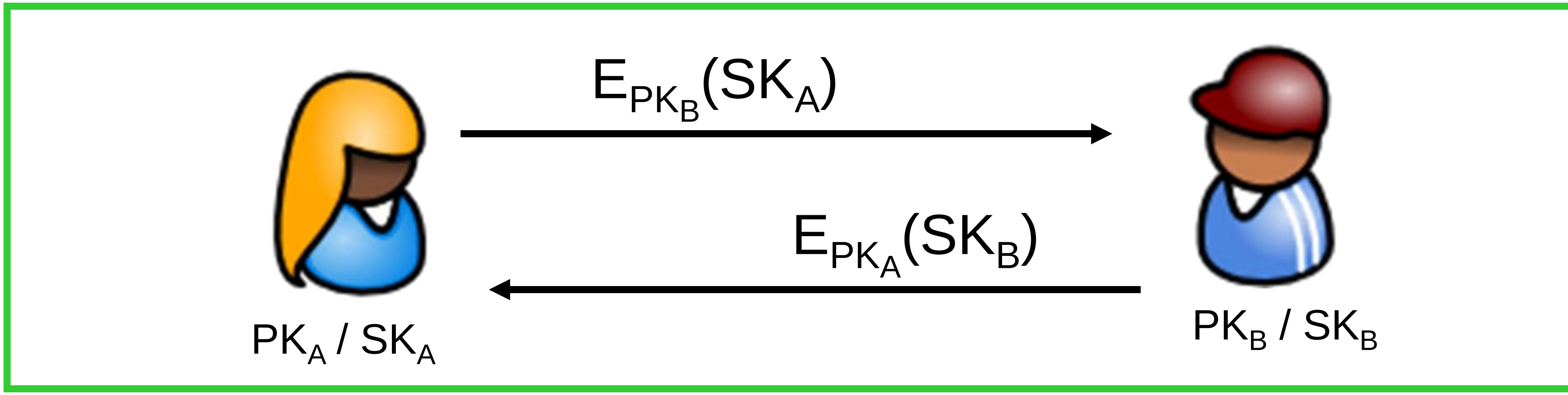


- <u>P2P file storage</u>: [BDET'00]
  - Goal: file enc is independent of who created it
  - Method: **file-key ← hash(file-contents)**

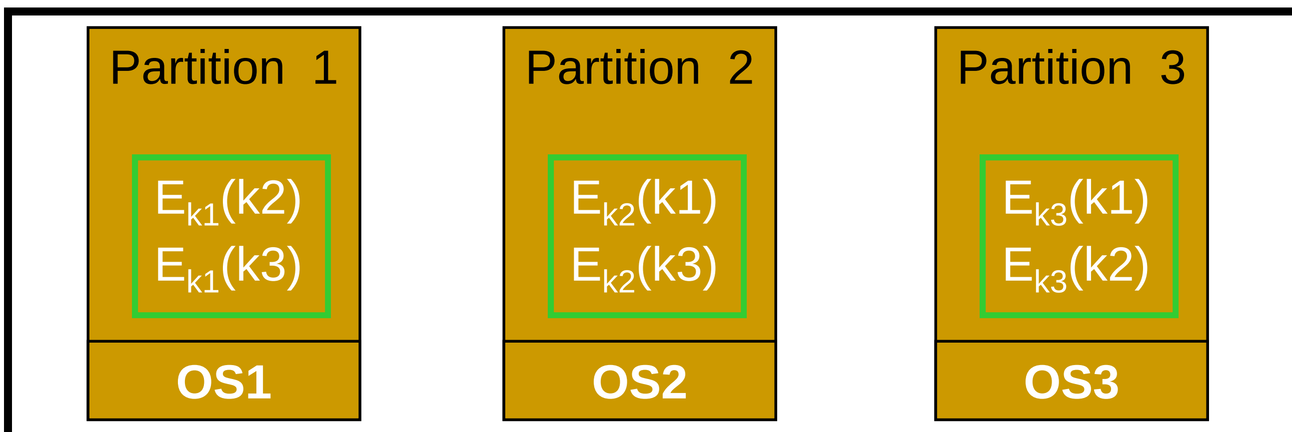
    ⇒ dependence between message and key

KDM in practice

- Collaboration:

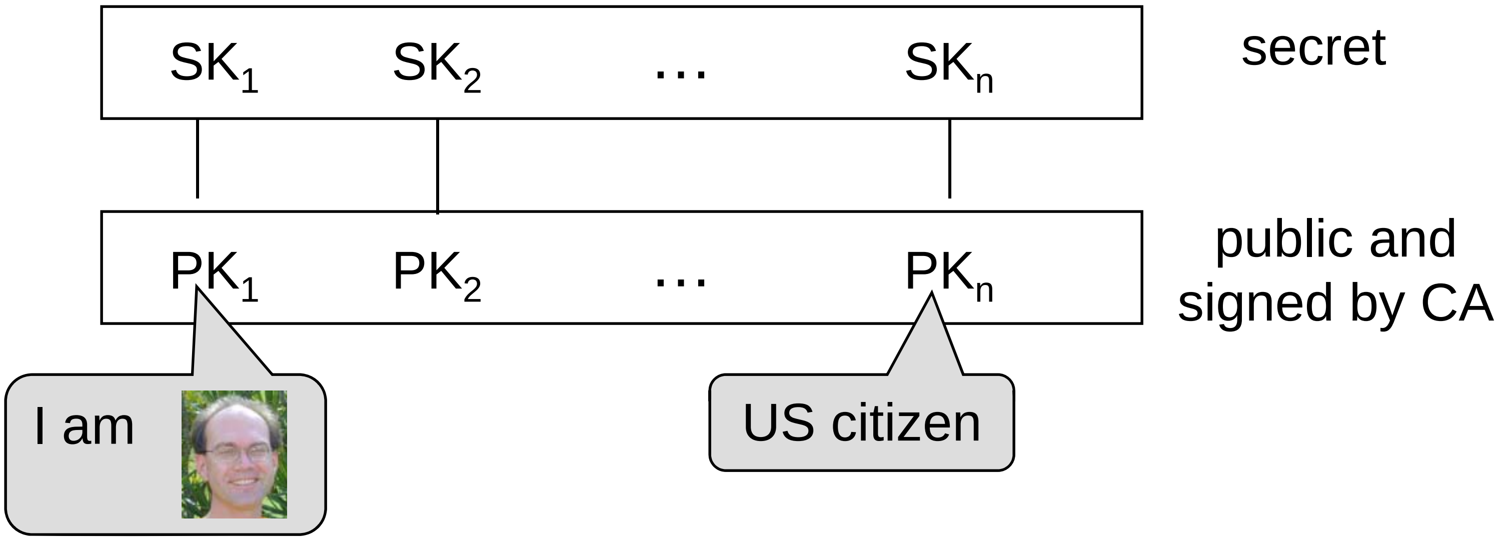


- Volume encryption with multiboot: (clique-encryption)



A Circular-Encryption Application [CL'01]

- A user has n credentials signed by CA:

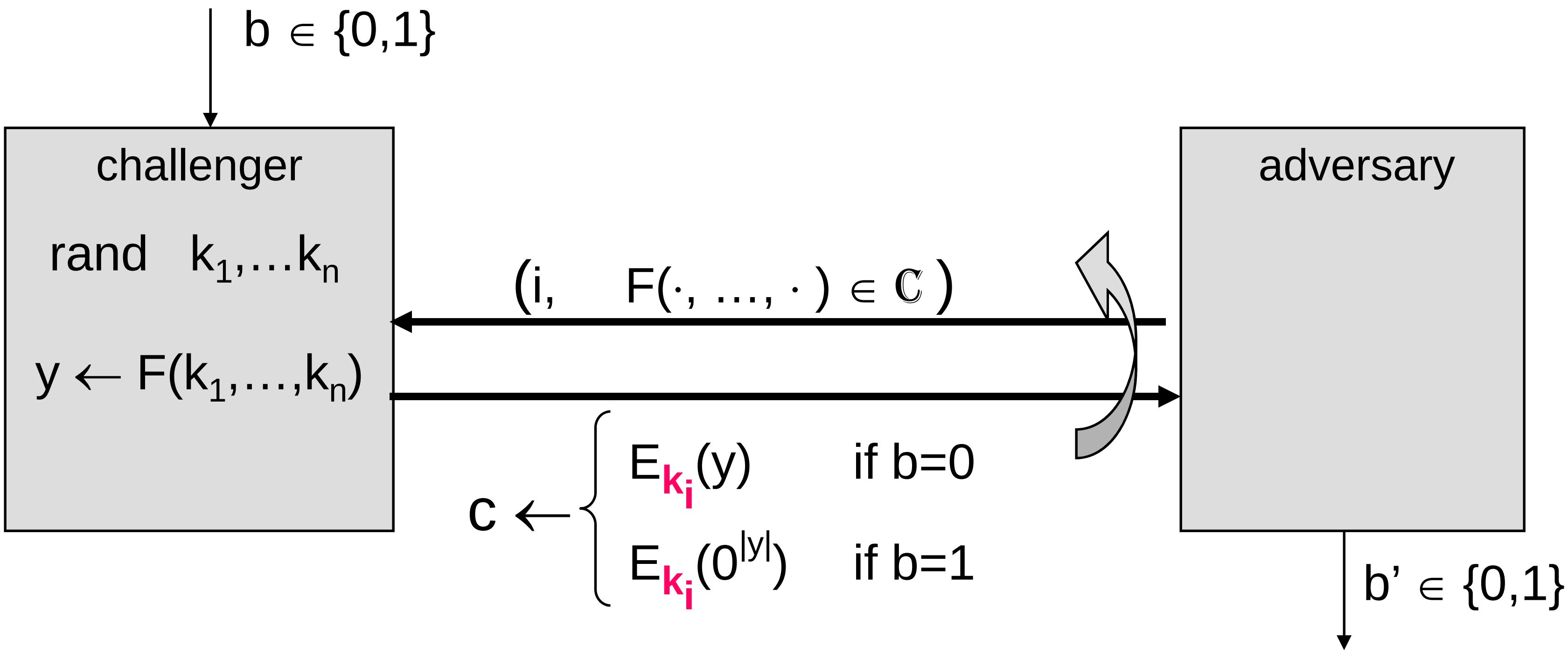


- User should not "lend" any of his credentials to a friend
- Solution [CL'01] : CA forces user to publish

$$E_{PK_1}[SK_2]\ ,\quad E_{PK_2}[SK_3]\ ,\quad \ldots\ ,\quad E_{PK_n}[SK_1]$$

KDM security: known results

- <u>New security model</u> [BRS'02]



Cipher is **$\mathbb{C}$-KDM secure** if $\left|\Pr[b=b'] - 1/2\right|$ is "negligible"

KDM security: known results

- **Selector** functions sufficient for circular security

  $F_i(x_1, \ldots, x_n) = x_i$ for $i=1,\ldots,n$

  adversary obtains $E_{k_i}(k_j)$ for all $1 \le i, j \le n$

- Open problem: KDM-secure system for non-trivial set $\mathbb{C}$

- KDM-security in the random-oracle model [BRS'02, CL01]

$$E_k(m) = \begin{cases} r \leftarrow \text{random in } \{0,1\}^{\kappa} \\ c \leftarrow [\, r,\ H(k,r) \oplus m \,] \end{cases}$$

Is ElGamal circular secure?

- Let G be a group of order q , $1 \neq g \in G$
- KeyGen: $\mathbf{x \leftarrow \{1,\dots,q\}}$; $\mathbf{SK \leftarrow (x)}$; $\mathbf{PK \leftarrow (h=g^x)}$
- Encryption:

$$E_{PK}(m) = \begin{cases} r \leftarrow \text{random in } \{1,\dots,q\} \\ c \leftarrow [\, g^r \,,\; m \cdot h^r \,] \end{cases}$$

- Is ElGamal 1-circular secure ??

$$[\; h=g^x \,,\; \boxed{g^r \,,\; \mathbf{x} \cdot h^r} \;] \quad \text{indistin. from} \quad [\; h=g^x \,,\; \boxed{g^r \,,\; \mathbf{1} \cdot h^r} \;]$$

- Cannot reduce this to any standard hard problem …

New Results [BHHO'08]

- A variant of ElGamal with:

  KDM-security for all **affine** functions and

  based on the Decision Diffie-Hellman problem

- KeyGen: choose random $g_1 , \ldots , g_t \leftarrow G$

  choose random $s_1 , \ldots , s_t \leftarrow \{0,1\}$

  $PK = [\ g_1 , \ldots, g_t ,\ h= (g_1)^{s_1} \ldots (g_n)^{s_n}\ ]$

  $SK = [\ (g_1)^{s_1} , \ldots , (g_t)^{s_t}\ ]$

- Encryption:

  $E_{PK}(m) = [\ (g_1)^r , \ldots , (g_t)^r\ ,\ m \cdot h^r\ ]$

Proof idea: circular security

- Step 1: prove 1-circular security:

$$E_{PK}(SK) \quad \text{inditin. from} \quad E_{PK}(1)$$

- Step 2: 1-circular security $\Rightarrow$ n-circular security
  - Use "secret-key homomorphism"

$$PK_1, \quad E(PK_1, m), \quad \Delta \in \{0,1\}^t \quad \Rightarrow \quad PK_2, \quad E(PK_2, m)$$

$$SK_1 \qquad\qquad SK_2 = SK_1 \oplus \Delta$$

  - Building an n-wise encryption clique:

$$E(PK_1, SK_1) \Rightarrow E(PK_2, SK_1), \ \ldots, \ E(PK_n, SK_1)$$

Summary

- Encrypting key-dependent messages can be risky
  - often can and should be avoided
- Circular counter-examples illustrate the problem:
  - easy: 1-circular counter-example
  - harder: 2-circular counter-example [BHHO'08]
    - counter-example for weakly-secure systems
- Constructions:
  - In the random oracle model [BRS'02, CL'01]
  - First construction based on DDH [BHHO'08]

THE END