Bar Ilan Winter School, Feb. 2013

Broadcast Encryption:
Recent progress and Open problem

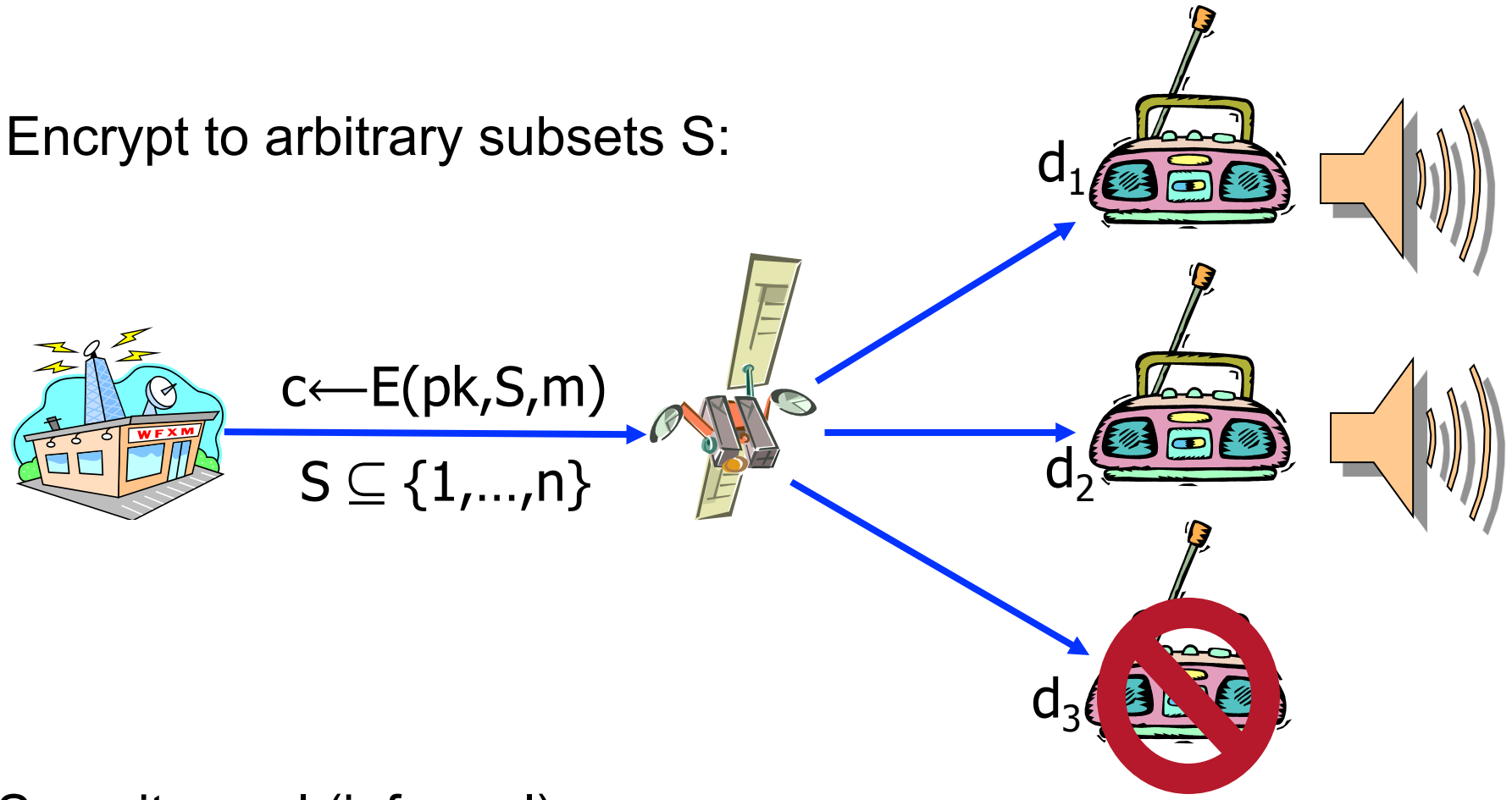
Dan Boneh

Stanford University

(1 hour)

Public-key Broadcast Encryption for Stateless Receivers [Fiat-Naor 1993]

Encrypt to arbitrary subsets S:



Security goal (informal):

Full collusion resistance: secure even if **all** users in S^c collude

Broadcast Encryption

Public-key BE system:

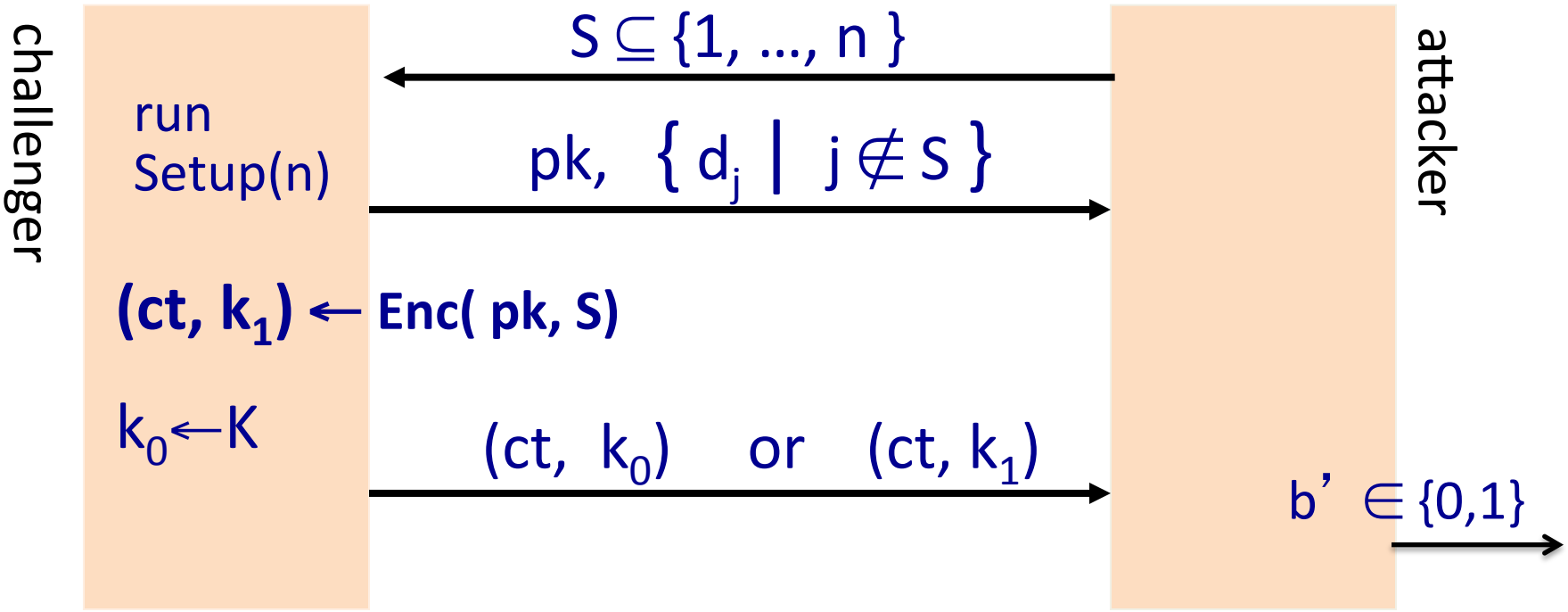
- **Setup**(n) $\longrightarrow$ pub. key **pk,** master sec. key **msk**
- **KeyGen(msk, j)** $\longrightarrow$ d_j (private key for user j)
- **Enc**(pk, S) $\longrightarrow$ **ct , k**

  k used to encrypt msg for users $S \subseteq \{1, \ldots, n\}$
- **Dec**(pk, d_j, S, ct): If $j \in S$, output **k**

Broadcast contains ([S], ct , $E_{SYM}(k, msg)$)

Broadcast Encryption: Static Security

Semantic security when users collude (static adversary)

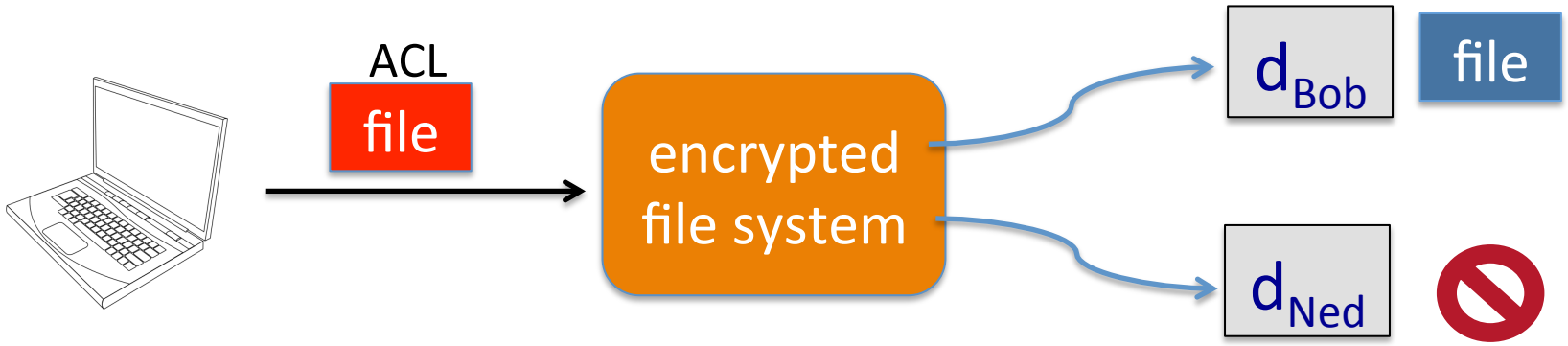


Def: Adv[A] = | Pr[b' is correct] - ½ |

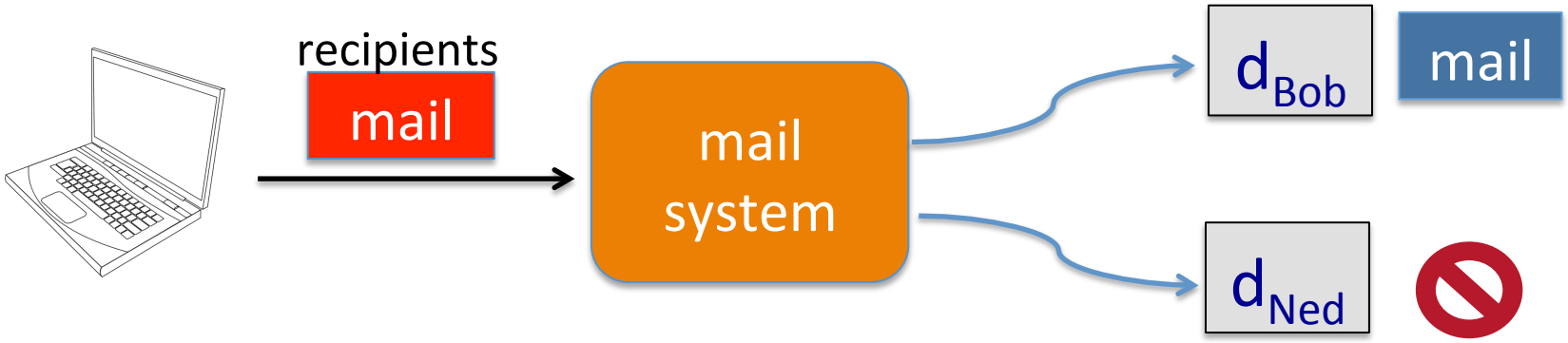
Security: ∀ poly-time A: Adv[A] is negligible

Broadcast systems are everywhere

File sharing in **encrypted file systems** (e.g. EFS):

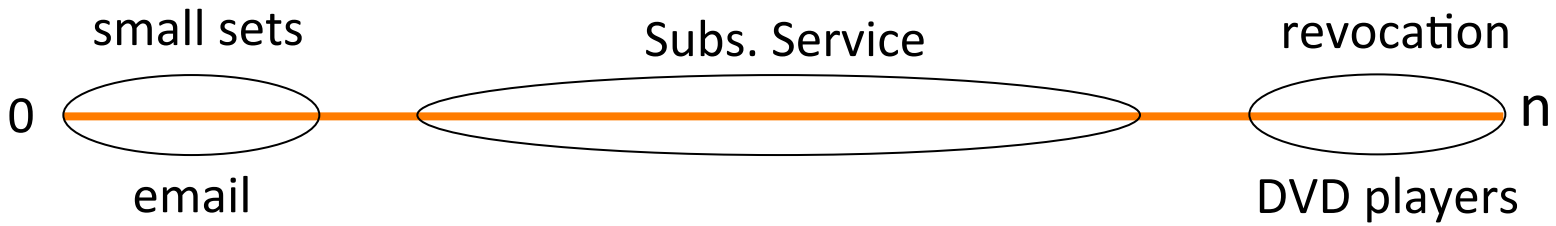


Encrypted mail system:



Social networks: privately send message to a group

Constructions



	|ct|	|sk|	|pk|
The trivial system:	**O(|S|)**	O(1)	O(n)
Revocation schemes: [NNL,HS,GST, LSW,DPP,…]	**O(n-|S|)**	O(log n)	O(1)

Can we have O(1) size ciphertext for all sets S ??

The BGW system: [B-Gentry-Waters'05]	**O(1)**	O(1)	O(n)

The BGW system

Setup(n): $g \leftarrow G$, α, **msk** $\leftarrow Z_q$, def: $g_k = g^{(\alpha^k)}$

$pk = (g, \; g_1, \; g_2, \ldots, g_n, \; g_{n+2}, \ldots, g_{2n}, \; v=g^{msk}) \in G^{2n+1}$

hole

KeyGen(msk, j) $\longrightarrow$ $d_j = (g_j)^{msk} \in G$

Enc(pk, S): $t \leftarrow Z_q$

$ct = \left(g^t, \; (v \cdot \prod_{j \in S} g_{n+1-j})^t \right)$, key = $e(g_n, g_1)^t$

Decryption

Decrypt(ct, S, d_u, pk): $ct = (c_0, c_1, c_2)$

$$e(g_u, c_1) / e\left(d_u \cdot \underbrace{\prod_{\substack{j \in S \\ j \neq u}} g_{n+1-j+u}}_{\text{precompute}}, c_0\right) = \underbrace{e(g_n, g_1)^t}_{\text{key}}$$

- If ΔS small, can easily update precomputation

Security

Thm: BGW is statically secure for n users in a bilinear group where n-DDHE assumption holds

n-DDHE: for rand. $g,h \leftarrow G$, $\alpha \leftarrow Z_q$, $R \leftarrow G_2$:

$$[\, h, g, g^{\alpha}, g^{(\alpha^2)},\ldots,g^{(\alpha^n)}, g^{(\alpha^{n+2})},\ldots,g^{(\alpha^{2n})}, e(g,h)^{(\alpha^{n+1})} \,]$$

$$\approx_p$$

$$[\, h, g, g^{\alpha}, g^{(\alpha^2)},\ldots,g^{(\alpha^n)}, g^{(\alpha^{n+2})},\ldots,g^{(\alpha^{2n})}, R \,]$$

Extensions, Variations, Improvements

Adaptive security: **[GW'10, PPSS'12, …]**

- Adversary can adaptively select what keys to request

Identity-based: **[SF'07, D'07, GW'10, …]**

- Smaller pubic key size: $|pk| = O(\text{maximal } |S|)$

  $\Rightarrow$ Set of all users can be $\{0, 1, 2, 3, \ldots, 2^{256}\}$

Chosen ciphertext secure: **[BGW'05, PPSS'12, …]**

Trace & revoke: **[BW'06]**

k-linear maps: a recent breakthrough

S. Garg, C. Gentry, S. Halevi



Properties: (informal)

- Representation of $g \in G$ is $O(k)$ bits
- Better than k-linear map: **gradation**

$e_1: G \times G \longrightarrow G_2$

$e_2: G \times G_2 \longrightarrow G_3$

$\vdots$

$e_k: G \times G_k \longrightarrow G_{k+1}$

For our purposes:

$e_k: G \times \cdots \times G \longrightarrow G_k$

$e: \; G_k \times G_k \longrightarrow G_{2k}$

BGW using (log n)-linear map

Recall: BGW Setup(n): $g \leftarrow G$, α, **msk** $\leftarrow Z_q$. pk:

$$g,\quad g^{\alpha}, g^{(\alpha^2)},\ldots, g^{(\alpha^n)},\quad g^{(\alpha^{n+2})},\ldots,g^{(\alpha^{2n})},\quad v=g^{msk}$$

Suppose: $e_k: G\times\cdots\times G \longrightarrow G_k$; $e: G_k \times G_k \longrightarrow G_{2k}$

Set pk as: (#users $\approx 2^{k-1}$)

$$g,\quad g^{\alpha}, g^{(\alpha^2)}, g^{(\alpha^4)}\ldots, g^{(\alpha^{(2^{2k})})}, g^{(\alpha^{(2^{2k+1})})},\quad v=g_k^{msk}$$

Using e_k: can build all needed elements in pk

but for rand. $h\in G$ cannot build $e(g,\ldots,g,h)^{(\alpha^{(2^{2k-1})})} \in G_{2k}$

BGW using (log n)-linear map

	|ct|	|sk|	|pk|
Bilinear BGW: [B-Gentry-Waters'05]	**O(1)**	O(1)	O(n)
(log n)-linear BGW:	**O(log n)**	O(log n)	$O(\log^2 n)$

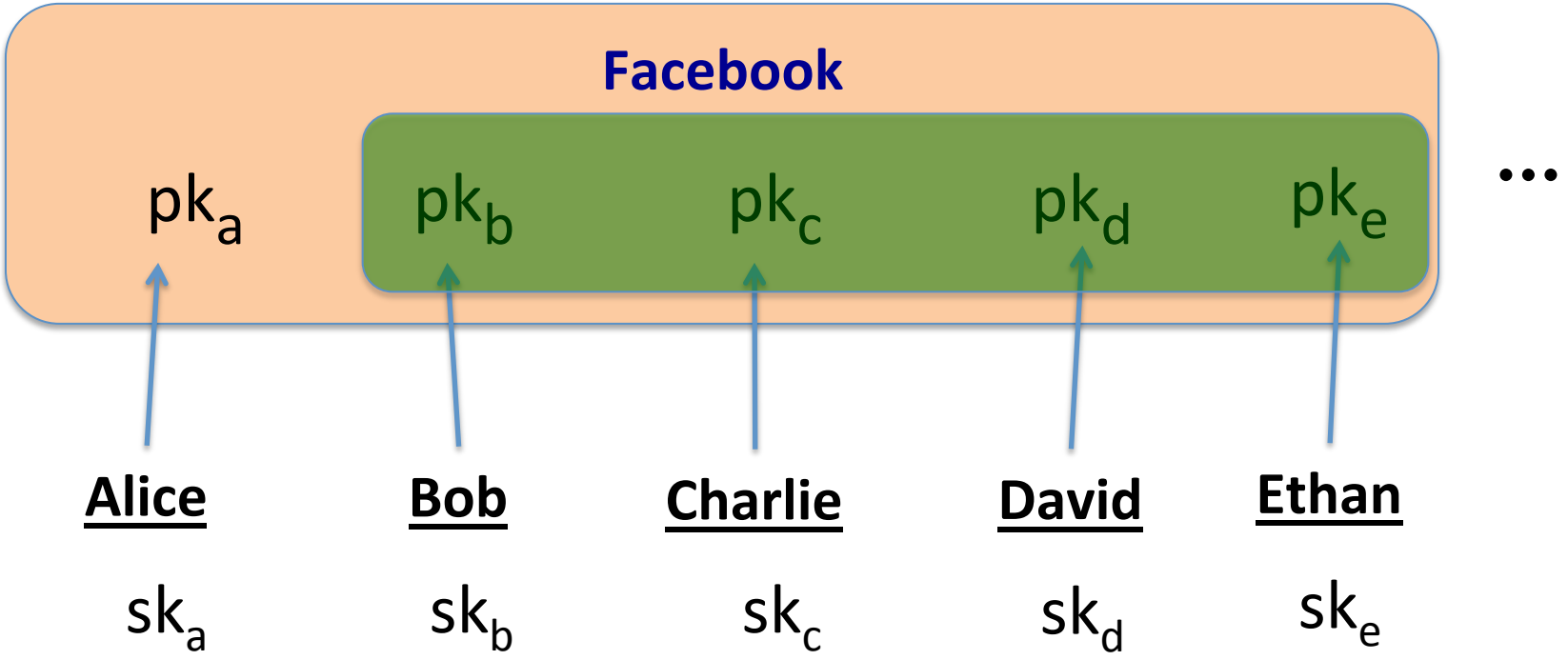
Open questions:

- Same parameters without k-linear maps ??
- O(1) size ct from standard lattice assumptions (LWE) ??

Distributed Broadcast Encryption?

Distributed Broadcast Encryption?

(users generate keys for themselves)

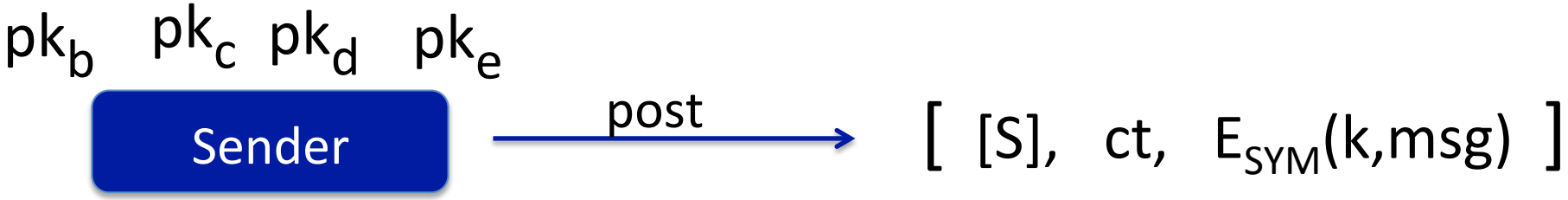


Sender → post → [[S], ct, E_{SYM}(k,msg)]

Distributed Broadcast Encryption?

The trivial system is distributed, but $|ct| = O(|S|)$

Goal: $|ct| =$ sub-linear($|S|$)



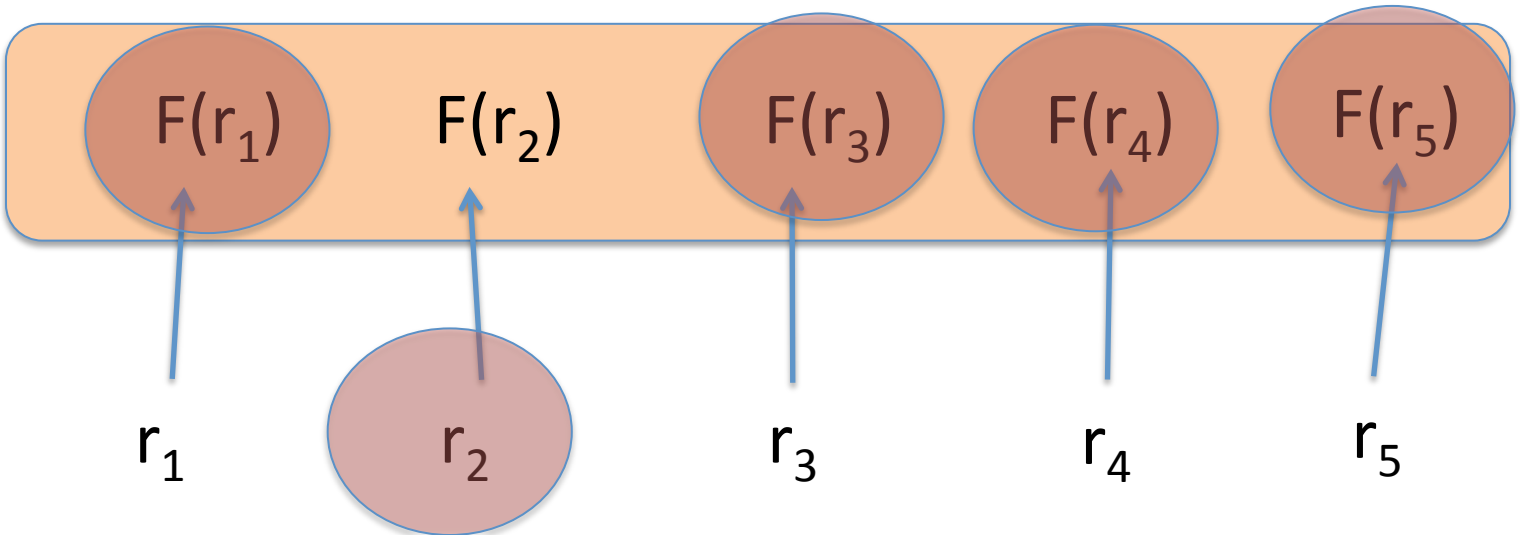
An approach: n-way DH [J'00, BS'03, GGH'12]

Def: an **n-way DH scheme** is a pair of det. algorithms (F, G)

$$F: R \longrightarrow Y \quad , \quad G: R \times Y^{n-1} \longrightarrow K$$

Correctness: $\forall\, r_1,\ldots,r_n$: $G\big(\, r_i,\ F(r_1), \ldots, \widehat{F(r_i)}, \ldots, F(r_n)\,\big) = K(r_1, \ldots, r_n)$

Security: given $F(r_1), \ldots, F(r_n)$: $K(r_1, \ldots, r_n) \approx_p$ uniform(K)

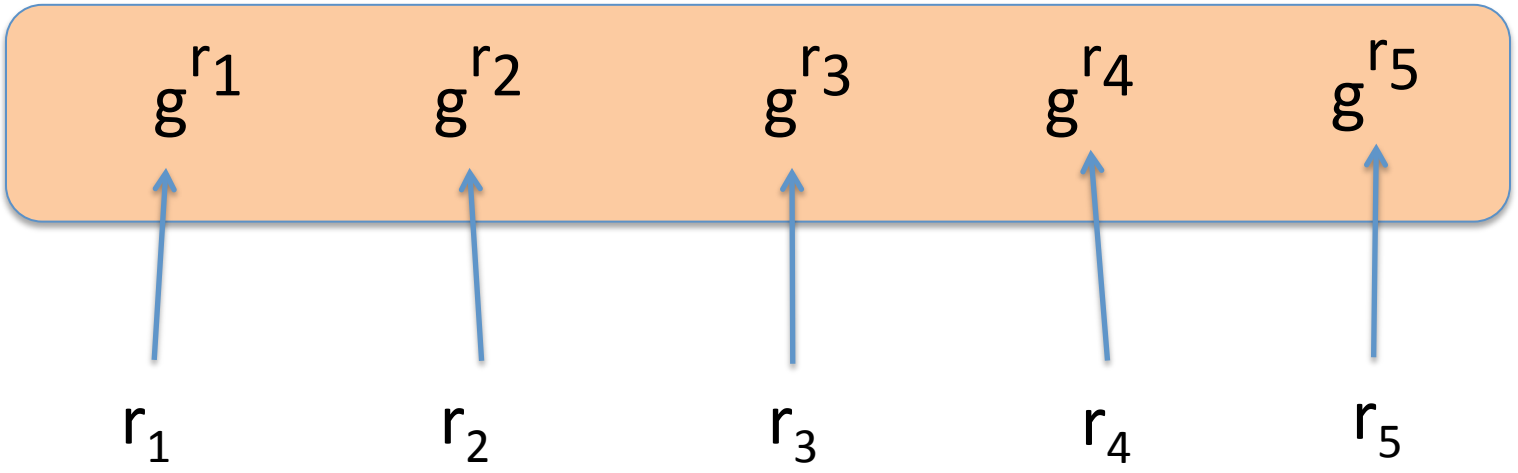


n-way DH: example [J'00, BS'03, GGH'12]

Example (Joux'00): $e_{n-1}: G \times \cdots \times G \longrightarrow G_{n-1}$

$F(r) := g^r$; shared key = $e_{n-1}(g, \ldots, g)^{r_1 r_2 \cdots r_n}$

$G(r_1, g^{r_2}, \ldots, g^{r_n}) := e(g^{r_2}, \ldots, g^{r_n})^{r_1}$

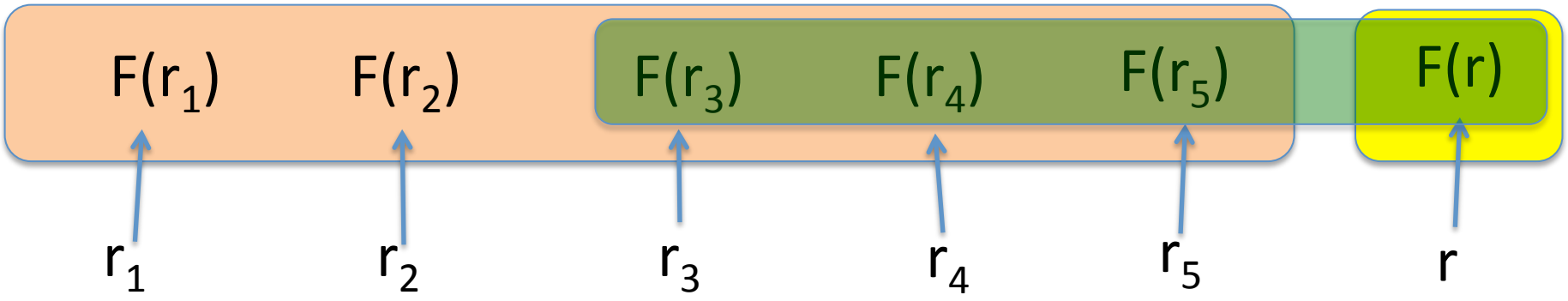


n-way DH ⇒ distrib. BE

KeyGen(i): $sk_i \leftarrow R$, $pk_i = F(sk_i) = g^{sk_i}$

Enc(S , $\{ pk_i \}_{i \in S}$): choose $r \leftarrow R$

output $ct = F(r) = g^r$, $key = G_{|S|+1}(r, \{ pk_i \}_{i \in S})$



Problem: bit-size of g^r is O(n)

Is there a distributed BE where |ct| is sub-linear(|S|) ??

Private broadcast encryption

Private broadcast encryption [BBW'06, LPQ'12]

Privacy violations in many implementations:

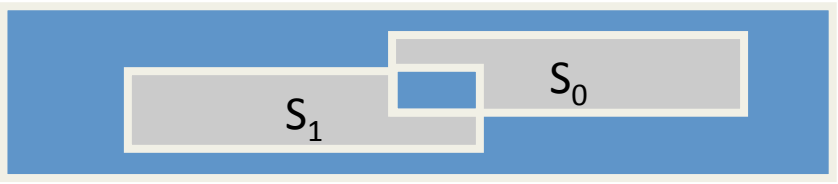
- Windows EFS.
- BCC in S/MIME: Outlook, Thunderbird, …
- BCC in PGP

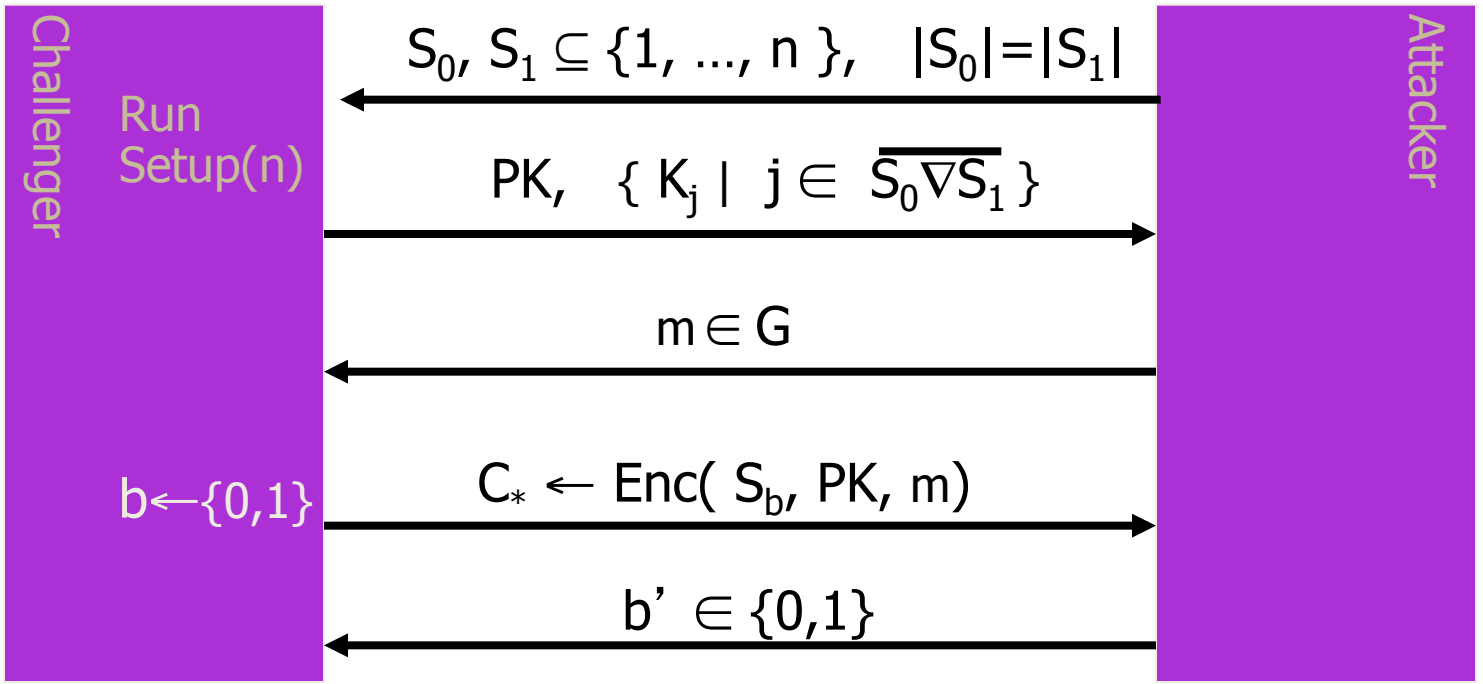
Reason: CT header reveals recipient set.

Solution: broadcast ciphertext should conceal recipient set S (but not its size)

$\Rightarrow$ private broadcast encryption

Private Broadcast Encryption [BBW' 06]





Def: Alg. A ε-breaks BE sem. sec. if $Pr[b=b'] > \frac{1}{2} + \varepsilon$

Constructions [BBW'04, LPQ'12]

- The trivial system (with anon. pub-key enc.)

  ciphertext size: $|S| \times$(sec. param.) , $O(|S|)$ decryption time

- Best known construction: [BBW'04]

  ciphertext size: $|S| \times$(sec. param.) , $O(\log|S|)$ dec. time

---

Open: private BE of ct. size sub-linear($|S|$) × (sec. param.) + $|S|$

- Fazio-Perera'12: NNL-like system, but only outsider privacy

Summary so far …

Many open problems in broadcast encryption:

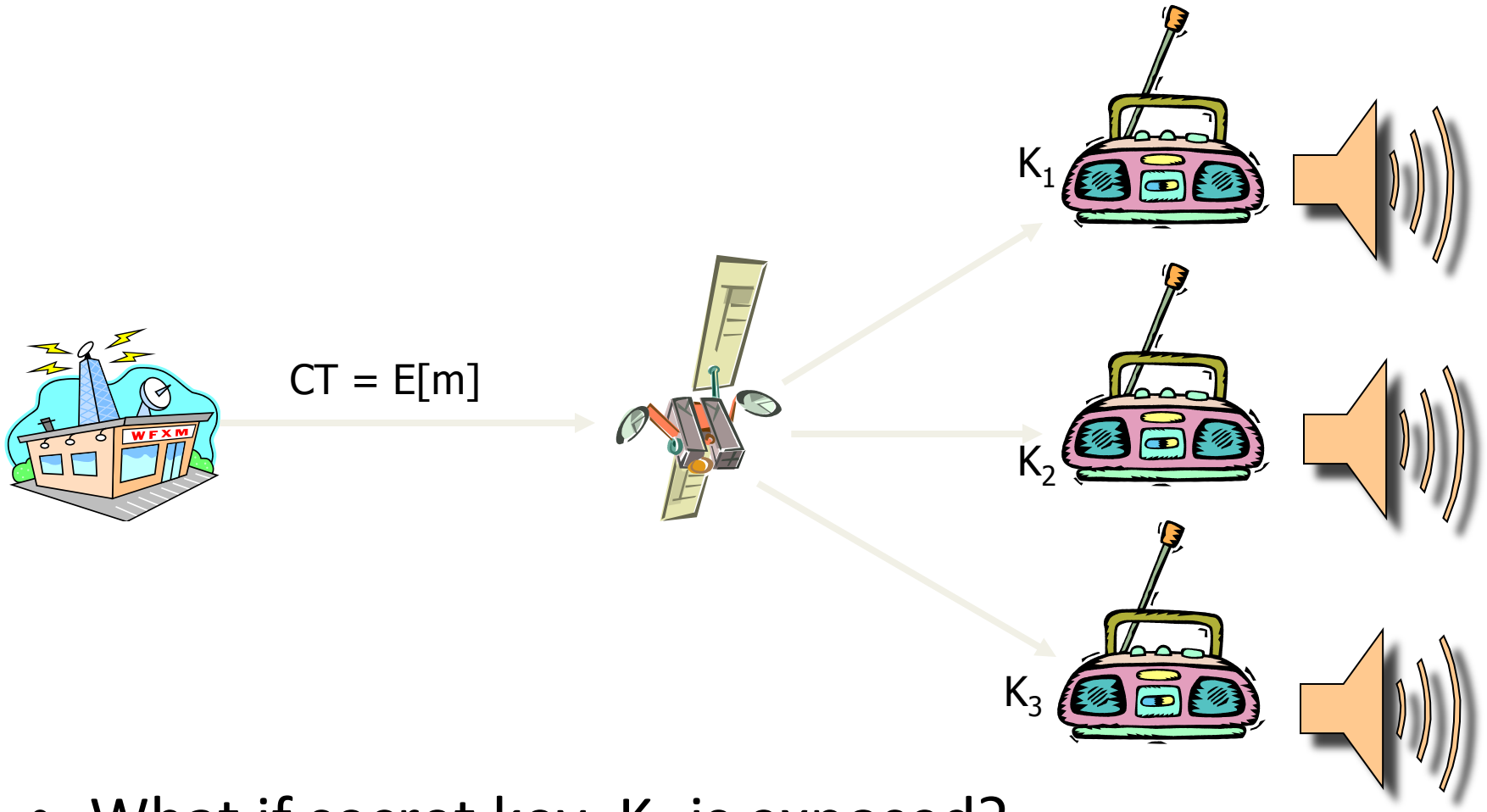
- O(log n) size ciphertext & secret keys from LWE?
- O(log n) size ct, sk, and pub-key w/o k-linear maps?
- Sub-linear (fully) private broadcast encryption?

  note: (linear) private BE ⇒ traitor tracing [BSW'05]

- Distributed BE with sub-linear ciphertext?

Part II: Traitor Tracing

Tracing Traitors [CFN' 94]



- What if secret key K_i is exposed?
  - Goal: Trace pirate decoder D to key K_u

    Then kill user u (or revoke his key)

Tracing Traitors

- Setup (n): outputs private keys $K_1, \ldots, K_n$
  public-key PK and tracer key TK.

  User i gets private key K_i

- Encrypt (PK, M) $\rightarrow$ ciphertext C

- Decrypt (K_i, C) $\rightarrow$ message M

- Trace ^{D} (TK) $\rightarrow$ $i \in \{1,\ldots,n\}$
  - Outputs index of at least one key used to build D
  - D is a stateless black-box pirate decoder.

Why black-box tracing? [BF' 99]

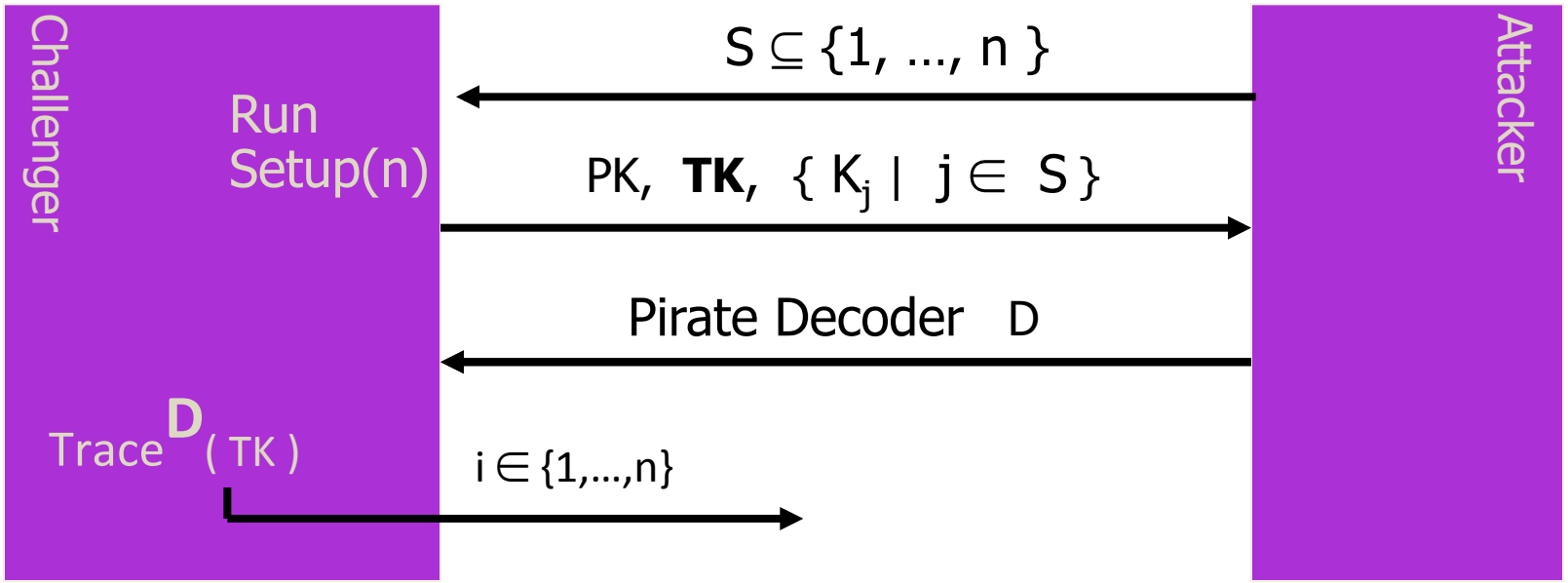
D: may contain unrecognized keys,
is obfuscated, or tamper resistant.

<u>All we know</u>:

$$\Pr[\, M \xleftarrow{R} G,\ \ C \xleftarrow{R} \text{Encrypt}(PK, M) \ :\ \ D(C)=M\,] \ > 1-\varepsilon$$

Formally: Secure TT systems

(1) Semantically secure, and (2) Traceable:



Adversary wins if: (1) $\Pr[D(C)=M] > 1-\varepsilon$, and

(2) $i \notin S$

Brute Force System

- Setup (n): Generate n PKE pairs (PK_i, K_i)

  Output private keys $K_1, \ldots, K_n$

  $PK \leftarrow (PK_1, \ldots, PK_n)$, $TK \leftarrow PK$.

- Encrypt (PK, M): $C \leftarrow (E_{PK_1}(M), \ldots, E_{PK_n}(M))$

- Tracing: next slide.

$\text{Trace}^{D}(PK)$: [BF99, NNL00, KY02]

For $i = 1, \ldots, n+1$ define for $M \xleftarrow{R} G$:

$$p_i := \Pr[\ D(\ E_{PK_1}(\perp), \ldots, E_{PK_{i-1}}(\perp), E_{PK_i}(M), \ldots, E_{PK_n}(M)\ ) = M\ ]$$

Then: $p_1 > 1-\varepsilon$; $p_{n+1} \approx 0$

$$1-\varepsilon = |p_{n+1} - p_1| = \left|\sum_{i=1}^{n} p_{i+1} - p_i\right| \le \sum_{i=1}^{n} |p_{i+1} - p_i|$$

$\Rightarrow$ exists $i \in \{1,\ldots,n\}$ s.t. $|p_{i+1} - p_i| \ge (1-\varepsilon)/n$

$\Rightarrow$ user i must be one of the pirates.

Security Theorem

Tracing algorithm estimates: $| \hat{p}_i - p_i | < (1-\varepsilon)/4n$

$\Rightarrow$ Need $O(n^2)$ samples per p_i. (D – stateless)

$\Rightarrow$ Cubic time tracing

(can be improved to quadratic in $|S|$)

Thm:

underlying PKE system is semantically secure

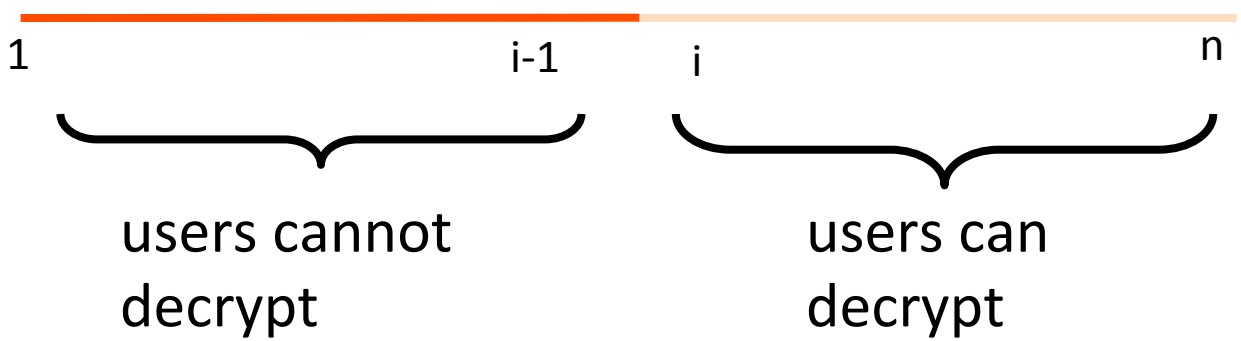
$\Rightarrow$

no eff. adv wins tracing game with non-neg adv.

Abstracting the Idea [BSW' 06]

Properties needed:

- For $i = 1, \ldots, n+1$ can encrypt M so:



Linear Broadcast Encryption

- Without K_i adversary cannot distinguish:

  Enc(i, PK, M) from Enc(i+1, PK, M)

Private B.E.

Private Linear Broadcast Enc (PLBE)

- Setup(n): outputs private keys $K_1, \ldots, K_n$ and public-key PK
- Encrypt(u, PK, M):
  encrypt M for users {u, u+1, …, n}
  output ciphertext CT.
- Decrypt(CT, j, K_j, PK): If $j \geq u$, output M

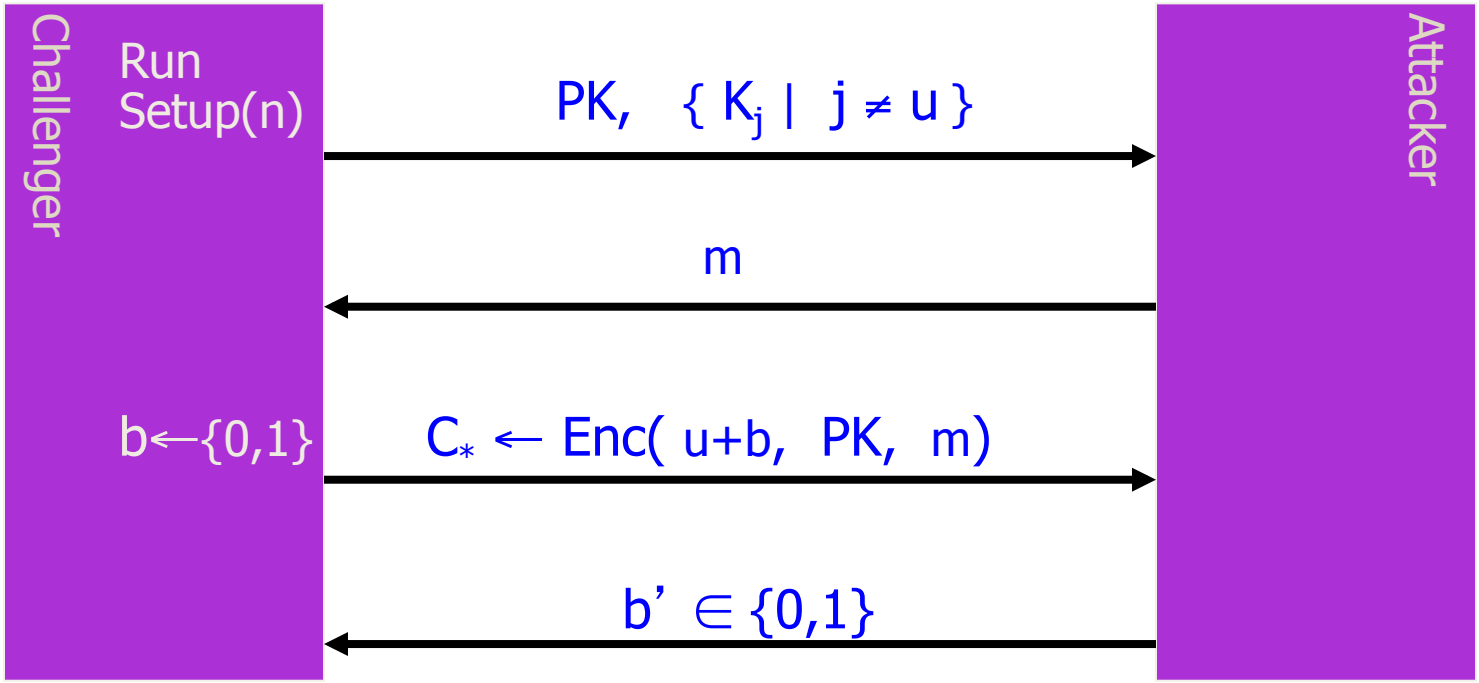
- Trace-Encrypt(PK,M) := Encrypt(1, PK, M)

Security definition

Message hiding: given all private keys:

$$\text{Encrypt}(n+1, M, PK) \approx_p \text{Encrypt}(n+1, \perp, PK)$$

Index hiding: for $u = 1, \ldots, n$:



Known Results

Thm: Secure PLBE $\Rightarrow$ Secure TT

Same size CT and priv-keys

(black-box and publicly traceable)

Best pairing-based PLBE system: [BSW'06]

CT-size = $O(\sqrt{n})$; priv-key size = $O(1)$

enc-time = $O(\sqrt{n})$; dec-time = $O(1)$

Improvements using k-linear maps?