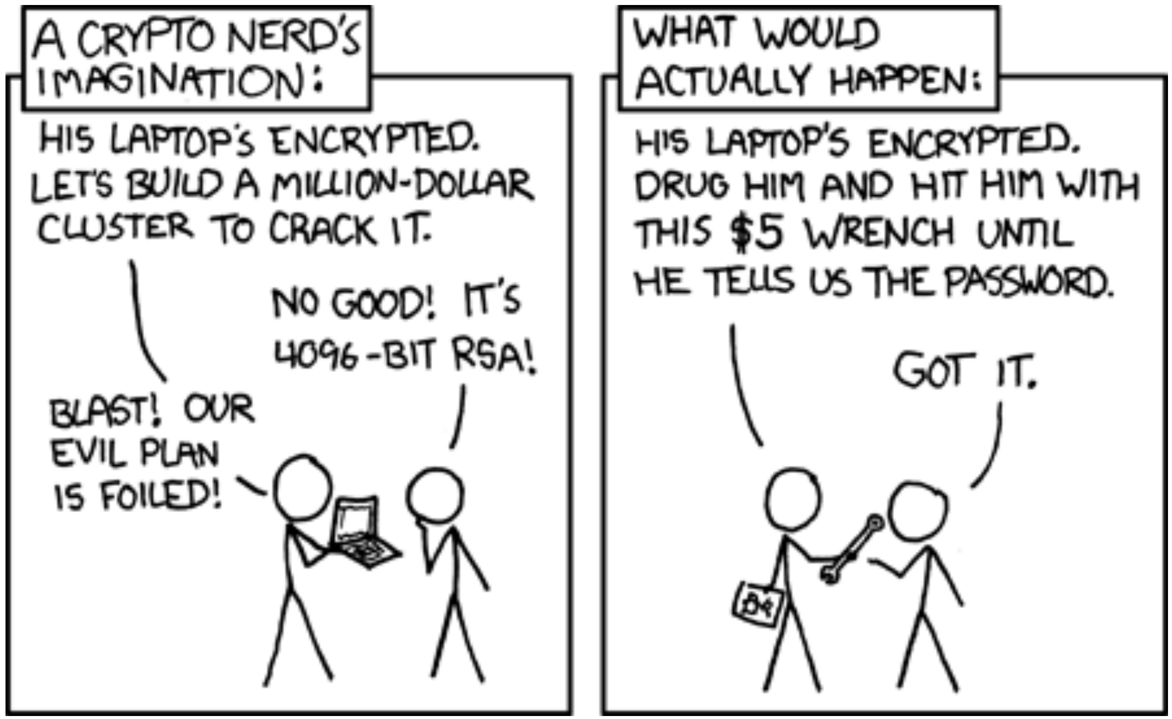
Asiacrypt 2012

$e: G \times G \longrightarrow G_2$

Pairings and Beyond

Dan Boneh
Stanford University

But first:
Rubber hose resistant cryptography



Source: XKCD

Psychology
Northwestern

Hristo Bojinov, Daniel Sanchez,

Paul Reber, Dan Boneh, Pat Lincoln

Rubber hose attacks

Problem:

authenticating users at the entrance to a secure facility

Current solutions:

- **Smartcards**: can be stolen
- **Biometrics**: can be copied or spoofed
- **Passwords**: can be extracted with a rubber hoze

Is there a non-extractable credential?

The human memory system

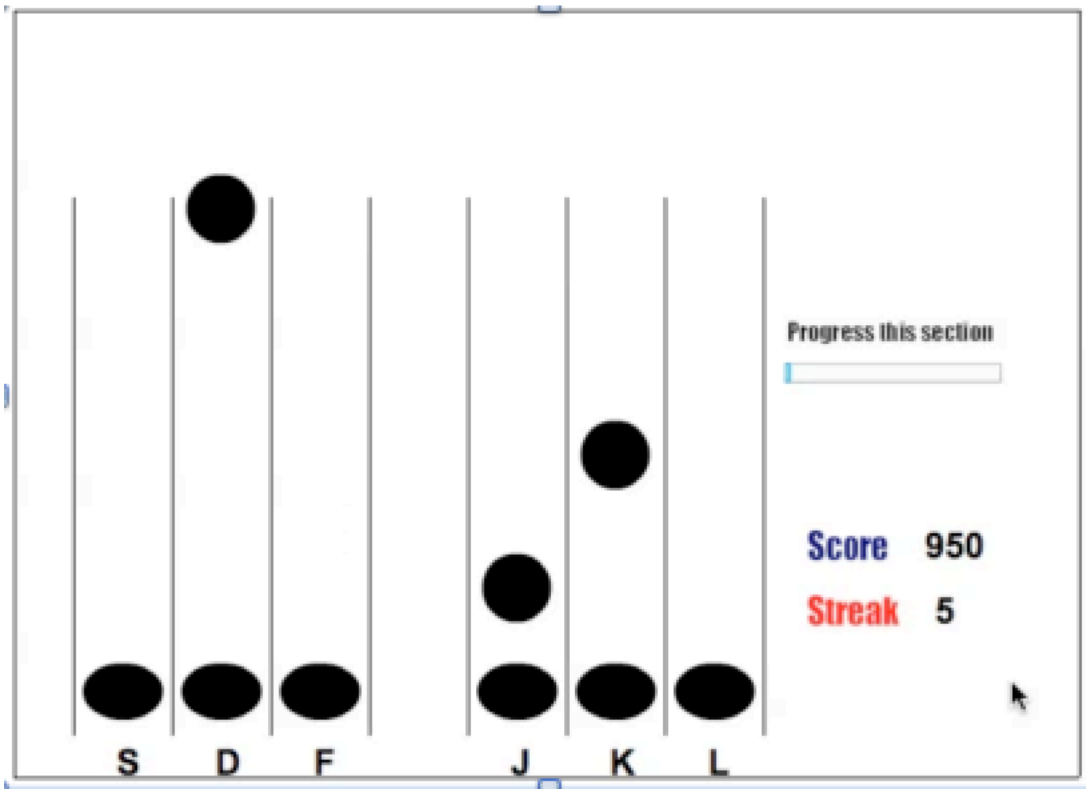
- **Hippocampus**: conscious learning
  - Learns from single examples
- **Basal ganglia**: “implicit learning”
  - Learns from many repeated samples

Our work: use implicit learning to teach a credential

- Credential can be tested at authentication time

  … but credential is not consciously accessible !!

Implicitly learning a credential



Participants exhibit essentially no recognition after training

Challenge-Response

Challenge-response authentication?

- Credential is an algorithm
- Given challenge, user computes response

What algorithms can we teach the Basal Ganglia?

- How does it represent knowledge?
- Is it complex enough for one-way functions?

… now back to bilinear maps

G , G_2 : finite cyclic groups of prime order q

An admissible bilinear map $e: G \times G \rightarrow G_2$ is:

- Bilinear: $e(g^a, g^b) = e(g,g)^{ab}$ $\forall a,b \in Z$, $g \in G$
- Non-degenerate: g generates G_1 $\Rightarrow$ $e(g,g)$ generates G_2
- Efficiently computable

Several examples where Dlog in G believed to be hard

Many Applications: enc., sigs., NIZK, …

Simplest example: BLS signatures [B-Lynn-Shacham'01]

KeyGen: $sk = \text{rand. } x$ in Z_q , $pk = g^x \in G$

Sign(sk, m) $\longrightarrow$ $H(m)^x \in G$

$$e\left(g, H(m)^x\right) = e\left(g^x, H(m)\right)$$

verify(pk, m, sig) $\longrightarrow$ accept iff $e(g, \text{sig}) \stackrel{?}{=} e(pk, H(m))$

Thm: Existentially unforgeable under CDH in the RO model

Beyond bilinear maps: k-linear maps [BS'03]

k-linear map $e: \underbrace{G \times G \times \cdots \times G}_{k} \longrightarrow G_k$ non-degen. & efficient

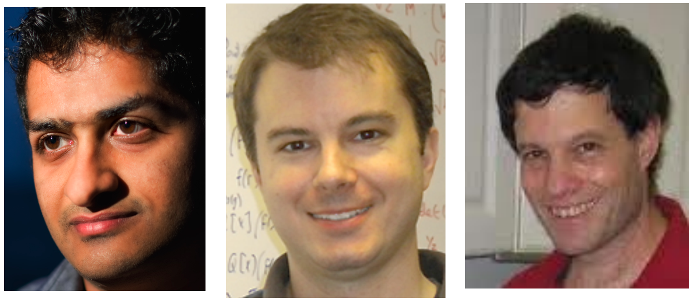
hard Dlog in G

Even more applications.

Can they be constructed?

k-linear maps: a recent breakthrough

S. Garg, C. Gentry, S. Halevi



Properties: (informal)

- The map $x \longrightarrow g^x$ is randomized
- 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:

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

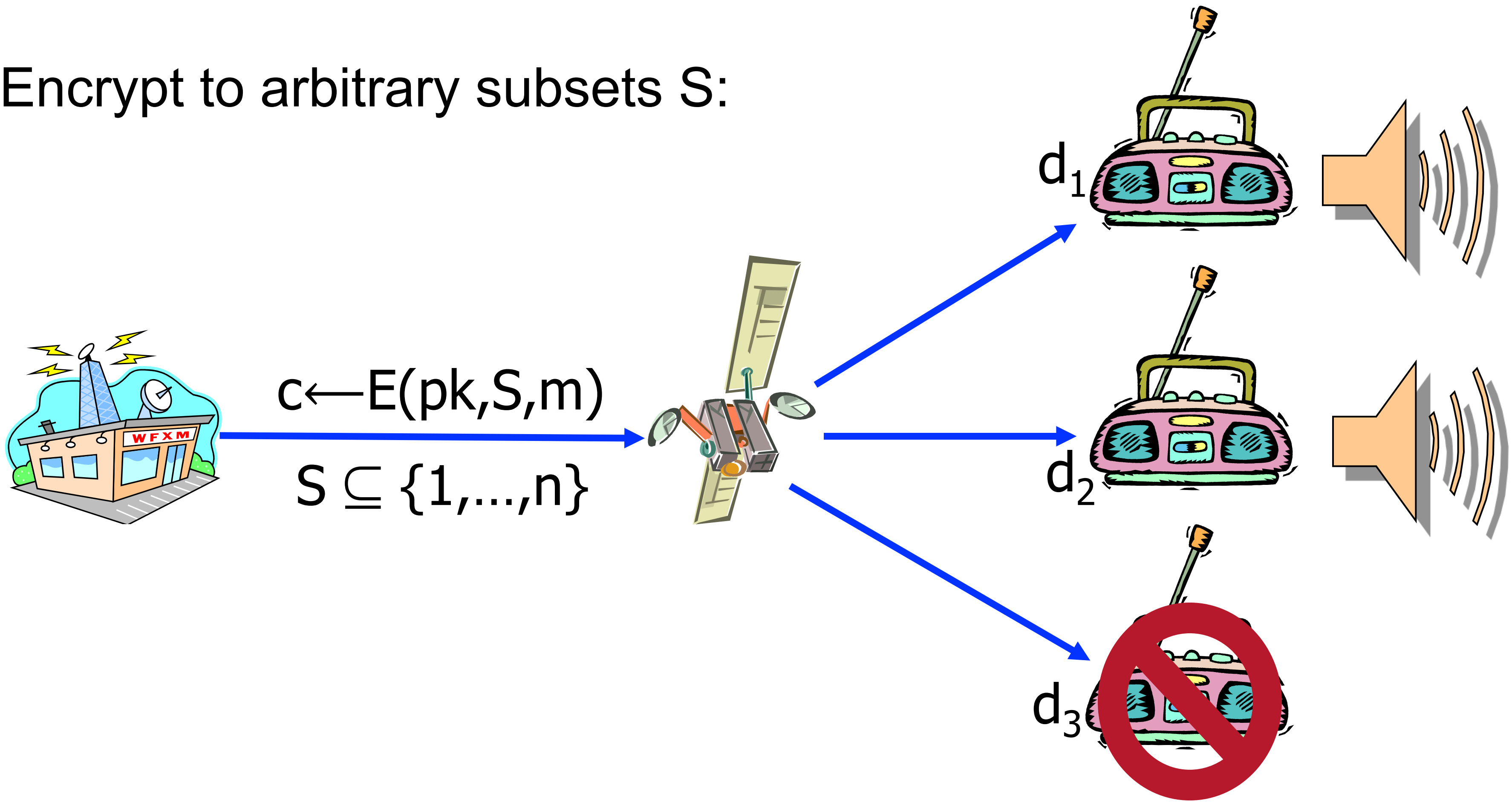
$e: \quad G_k \times G_k \longrightarrow G_{2k}$

Open Problems in Broadcast Encryption

(Public-key + Stateless receivers)

Broadcast Encryption [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**

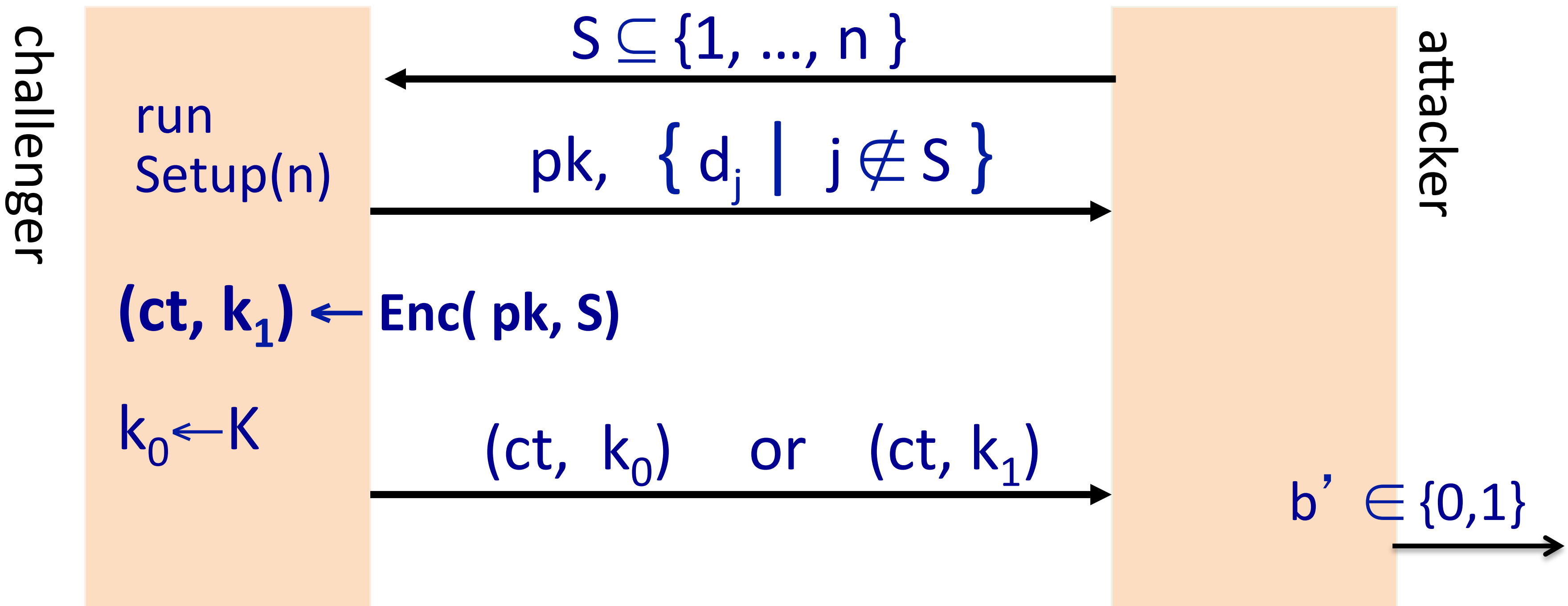
  k used to encrypt msg for users $S \subseteq \{1, ..., n\}$

- **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)

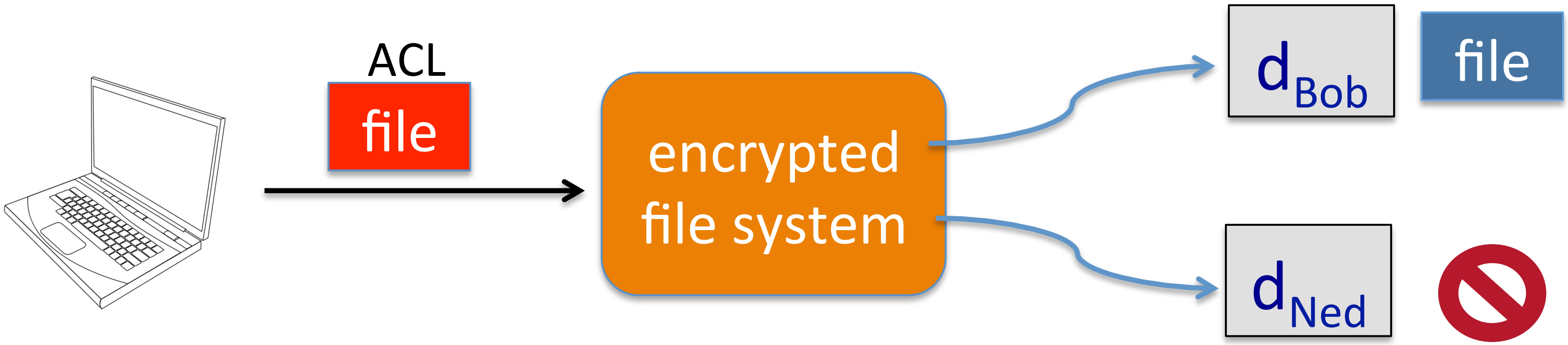


Def: $\text{Adv}[A] = \left| \Pr[\, b' \text{ is correct }] - \tfrac{1}{2} \right|$

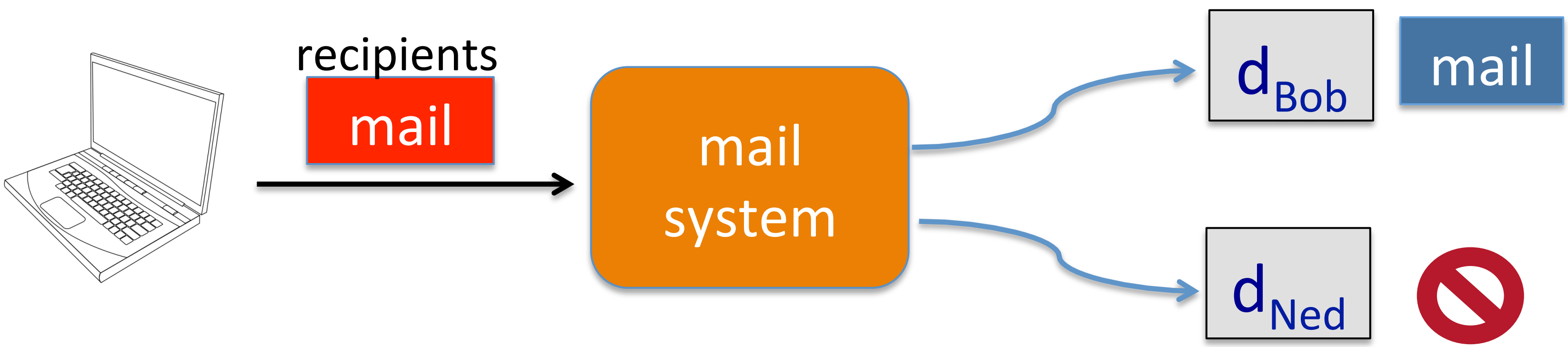
Security: ∀ poly-time A: Adv[A] is negligible

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

hole

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

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

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

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]

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 2k-linear map : 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

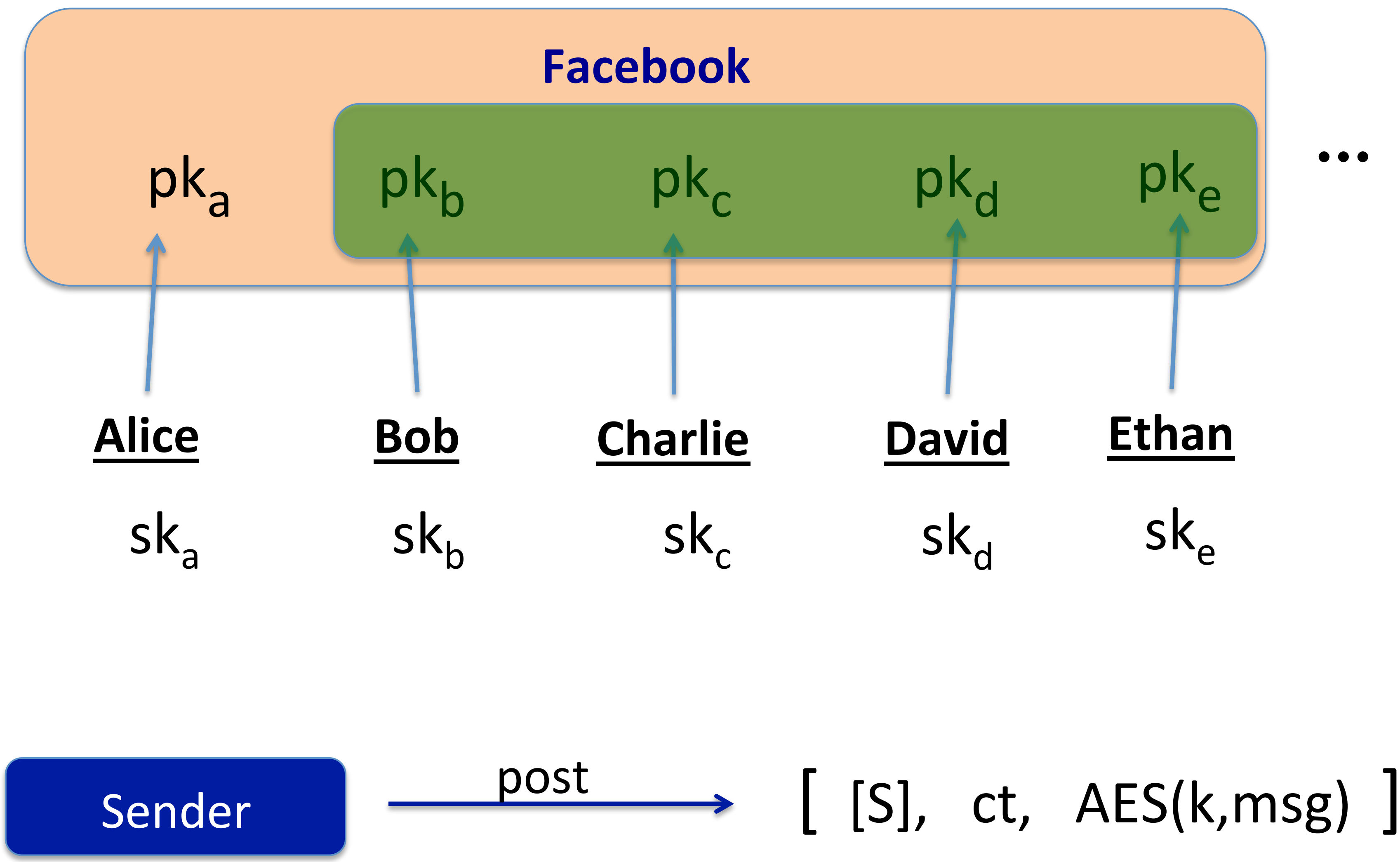
	|ct|	|sk|	|pk|
Bilinear BGW: [B-Gentry-Waters'05]	**O(1)**	O(1)	O(n)
(log n)-linear BGW:	**O(log n)**	O(log n)	$O(\log^2 n)$

Open questions:

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

Distributed Broadcast Encryption?

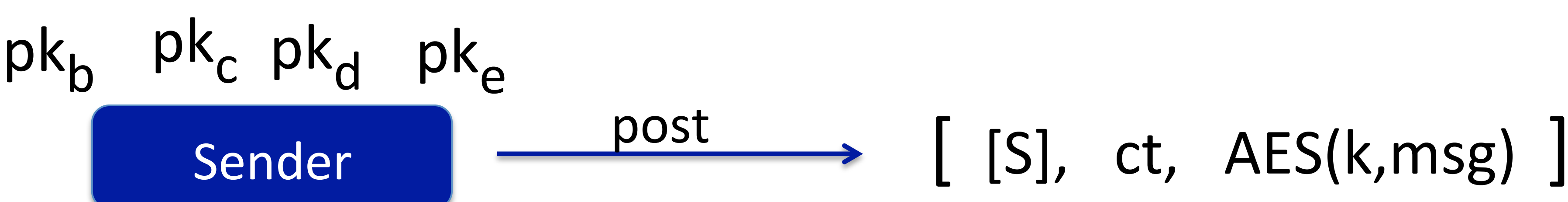
(users generate keys for themselves)



Distributed Broadcast Encryption?

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

Goal: $|ct| = \text{sub-linear}(|S|)$



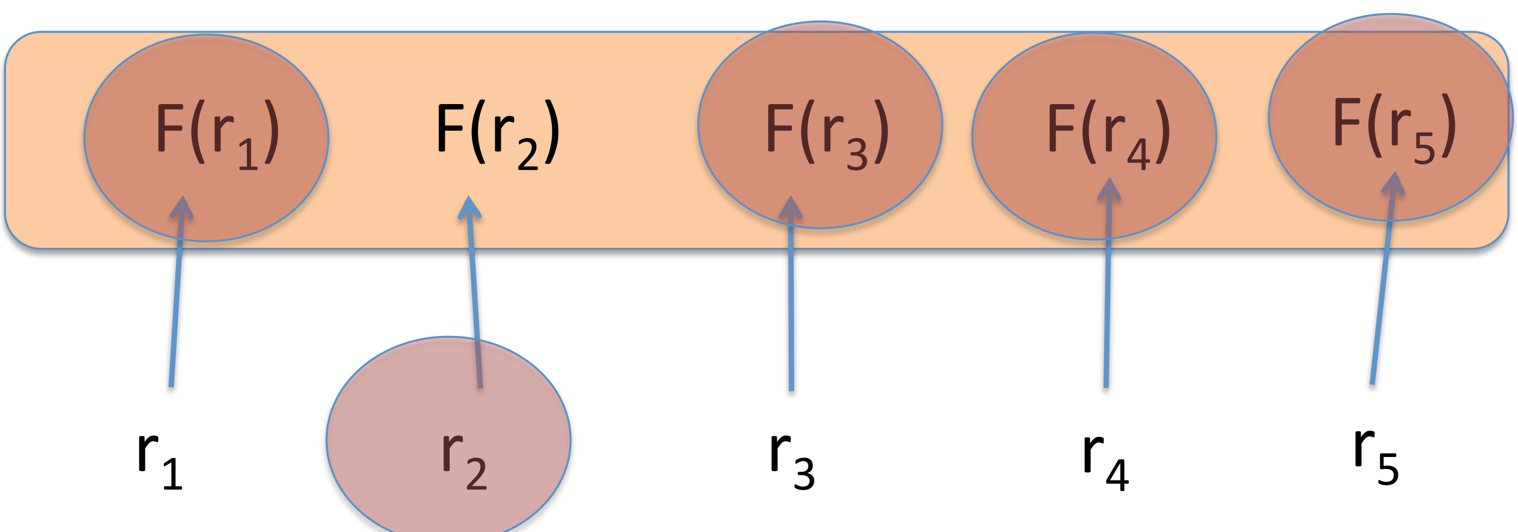
An approach: n-way DH [J'00, BS'03, GGH'12]

<u>Def</u>: 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 $F(r_1), \ldots, F(r_n)$: $K(r_1, \ldots, r_n) \approx_p \text{uniform}(K)$

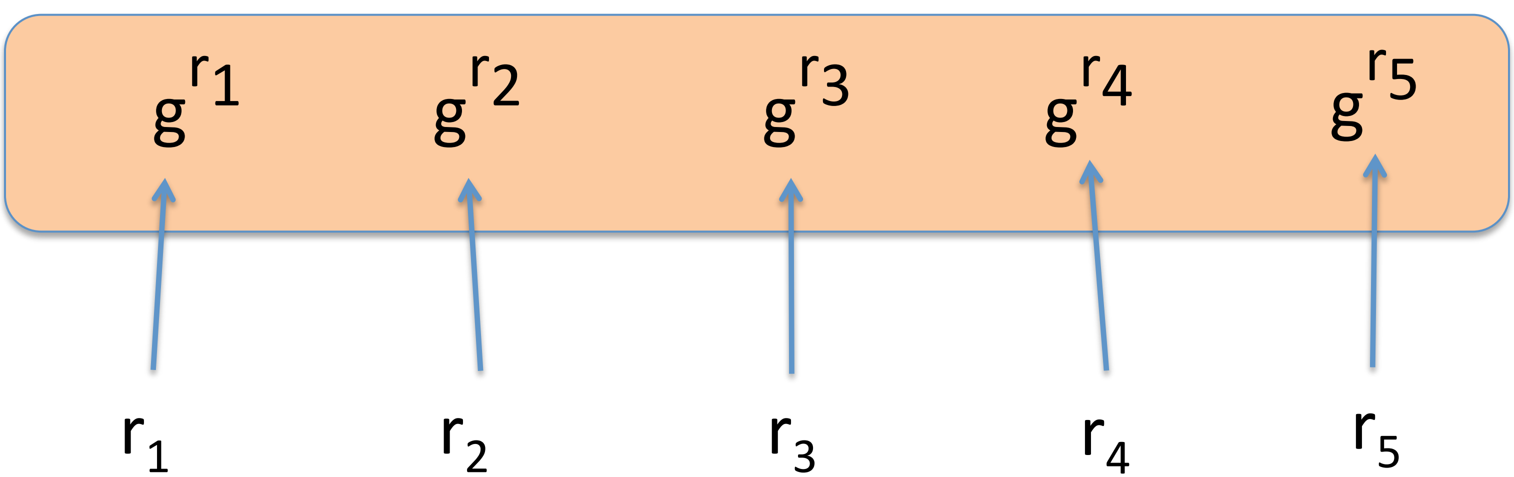


n-way DH: example [J’00, BS’03, GGH’12]

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

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

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

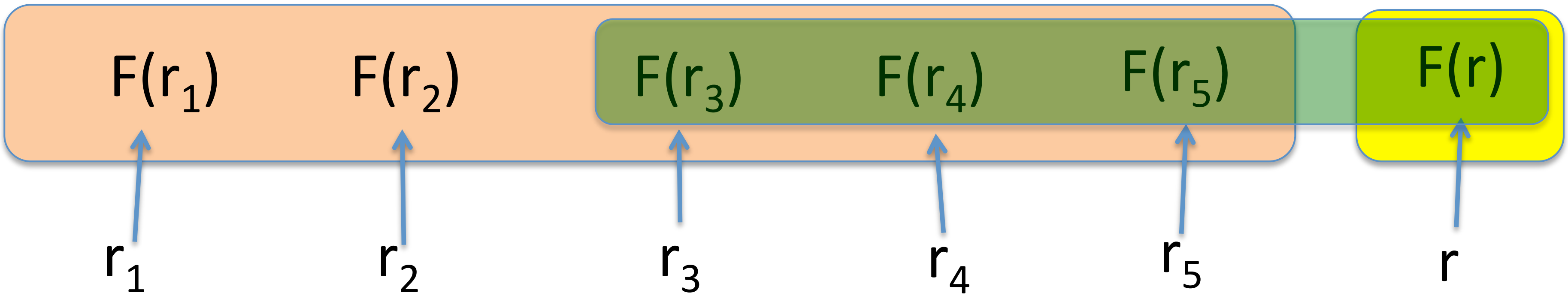


n-way DH ⇒ distrib. BE

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 [BBW'04, LPQ'12]

So far: broadcast ciphertext reveals recipient set S

Problem: encrypted mail systems

$\Rightarrow$ BCC recipients should not be revealed

Is there a BE system that hides the recipient set? (but not its size)

Example: the trivial system (with anon. pub-key enc.)

Best known constructions: ciphertext size $|S| \times$(sec. param.)

(and sub-linear decryption time)

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

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

Summary

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 $\Rightarrow$ traitor tracing [BSW'05]
- Distributed BE with sub-linear ciphertext?