

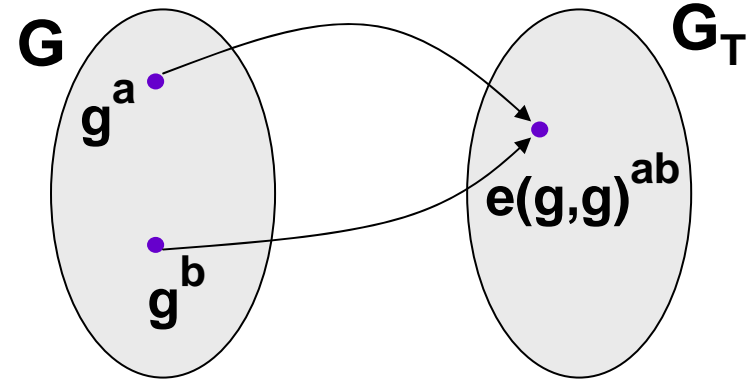


Bilinear Groups of Composite Order

Dan Boneh
Stanford University

Pairings $e: G \times G \rightarrow G_T$

- G, G_T : finite cyclic groups of **prime** order q .



- Pioneering work:
 - Menezes-Okamoto-Vanstone attack (IEEE '93)
 - Joux (ANTS '00),
 - Sakai-Ohgishi-Kasahara (SCIS '00)
- This talk: bilinear groups of **composite** order

Bilinear groups of order $N=pq$

[BGN'05]

- G : group of order $N=pq$. **(p, q) – secret**
bilinear map: $e: G \times G \rightarrow G_T$

$$G = G_p \times G_q. \quad g_p = g^q \in G_p \quad ; \quad g_q = g^p \in G_q$$

- Facts: $h \in G \Rightarrow h = (g_p)^a \cdot (g_q)^b$
 $e(g_p, g_q) = e(g^q, g^p) = e(g, g)^N = 1$
 $e(g_p, h) = e(g_p, g_p)^a \quad !!$

Example: supersingular curves

- To generate group G of order $N=pq$:
 - $p, q \leftarrow$ random odd primes
 - $N \leftarrow p \cdot q$
 - $L \leftarrow$ smallest prime in $\{ N-1, 2N-1, 3N-1, \dots \}$
where $L \equiv 3 \pmod{4}$

■ Let E/F_L be $y^2 = x^3 + x$

Then $E(F_L)$ has subgroup G of order N

$$e: G \times G \rightarrow (F_{L^2})^{((L^2-1)/N)}$$

-
- Non-supersingular examples using Cocks-Pinch [RS'06]

Applications

- This talk:
 - $(1+\varepsilon)$ Homomorphic encryption
 - Private Information Retrieval
 - Non-Interactive Zero Knowledge
 - Anonymous Identity Based Encryption
- Other:
 - Searching on encrypted data
 - Traitor Tracing
 - Group signatures
 - Mix nets with offline mixing

Homomorphic Encryption

BGN encryption

- KeyGen(λ): generate bilinear group G of order $N=p \cdot q$

$$PK \leftarrow (G, N, g, g_p) \quad ; \quad SK \leftarrow p$$

- Enc(PK, m): $r \leftarrow Z_N$, $C \leftarrow g^m (g_p)^r \in G$

- Dec(SK, C): $C^p = (g_q)^m \in G_q$
Output: $Dlog_{g_q}(C^p)$

- Note: decryption time is $O(\sqrt{m})$

\Rightarrow require small message space (e.g. $\{0,1\}$)

Homomorphic Properties

- $C_1 \leftarrow g^{m_1} (g_p)^{r_1}$, $C_2 \leftarrow g^{m_2} (g_p)^{r_2} \in G$

- Additive hom: $E(m_1+m_2) = C_1 \cdot C_2 \cdot (g_p)^s$

- **One** mult hom: $E(m_1 \cdot m_2) = e(C_1, C_2) \cdot e(g_p, g_p)^s$

- More generally: $E(m_1), \dots, E(m_n) \rightarrow E(F(m_1, \dots, m_n))$

For any $F \in \mathbb{Z}_N[X_1, \dots, X_n]$ of total degree 2

- Example: dot product on encrypted vectors

Security: the subgroup assumption

- Subgroup assumption:

$$\mathbf{G} \approx \mathbf{G}_p$$

Distribution $\mathbf{P}_G(\lambda)$:

$(G, g, p, q) \leftarrow \text{GroupGen}(\lambda)$

$N \leftarrow p \cdot q$

$s \leftarrow Z_N$

Output: (G, g, N, \mathbf{g}^s)

Distribution $\mathbf{P}_p(\lambda)$:

$(G, g, p, q) \leftarrow \text{GroupGen}(\lambda)$

$N \leftarrow p \cdot q$

$s \leftarrow Z_N$

Output: $(G, g, N, (\mathbf{g}_p)^s)$

For any poly-time A :

$$\left| \Pr[A(X) : X \leftarrow \mathbf{P}_G(\lambda)] - \Pr[A(X) : X \leftarrow \mathbf{P}_p(\lambda)] \right| < 1/\text{poly}(\lambda)$$

Thm: BGN is semantically secure under the subgroup assumption

Sample Applications:

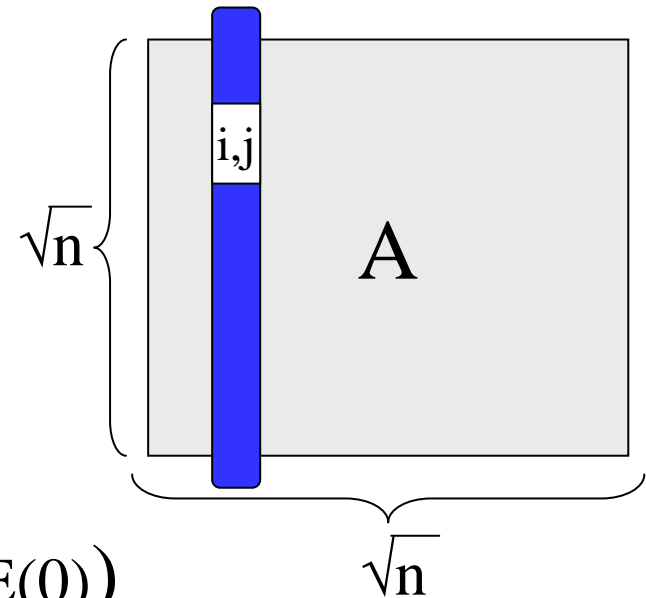
Private Information Retrieval

KO-PIR [KO'97]

- Use additively homomorphic encryption (e.g. Paillier)



$$(i, j) \in [\sqrt{n}]^2$$



1. Generate Paillier PK, SK

2. Send: $\text{PK}, E(\mathbf{u}_i) = (E(0), \dots, E(1), \dots, E(0))$

$(E(w_{i,1}), \dots, E(w_{i,\sqrt{n}})) \leftarrow E[A \cdot \mathbf{u}_i]$

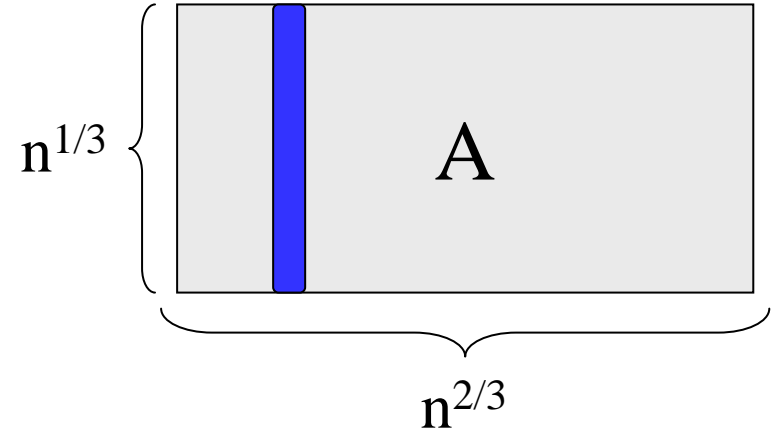
3. $D(\text{SK}, E(w_{i,j}))$

Total communication: $O(\sqrt{n})$

An improvement with composite groups



$$(i, j, k) \in [n^{1/3}]^3$$



1. Generate BGN PK, SK

2. Send: $\xrightarrow{\text{PK, } E(\mathbf{u}_i), E(\mathbf{u}_j)}$

$$E(\mathbf{v}_{i,j}) \leftarrow E(\mathbf{u}_i) \otimes E(\mathbf{u}_j)$$

$$\xleftarrow{(E(w_{i,j,1}), \dots, E(w_{i,j,n^{1/3}}))} E[A \cdot \mathbf{v}_{i,j}]$$

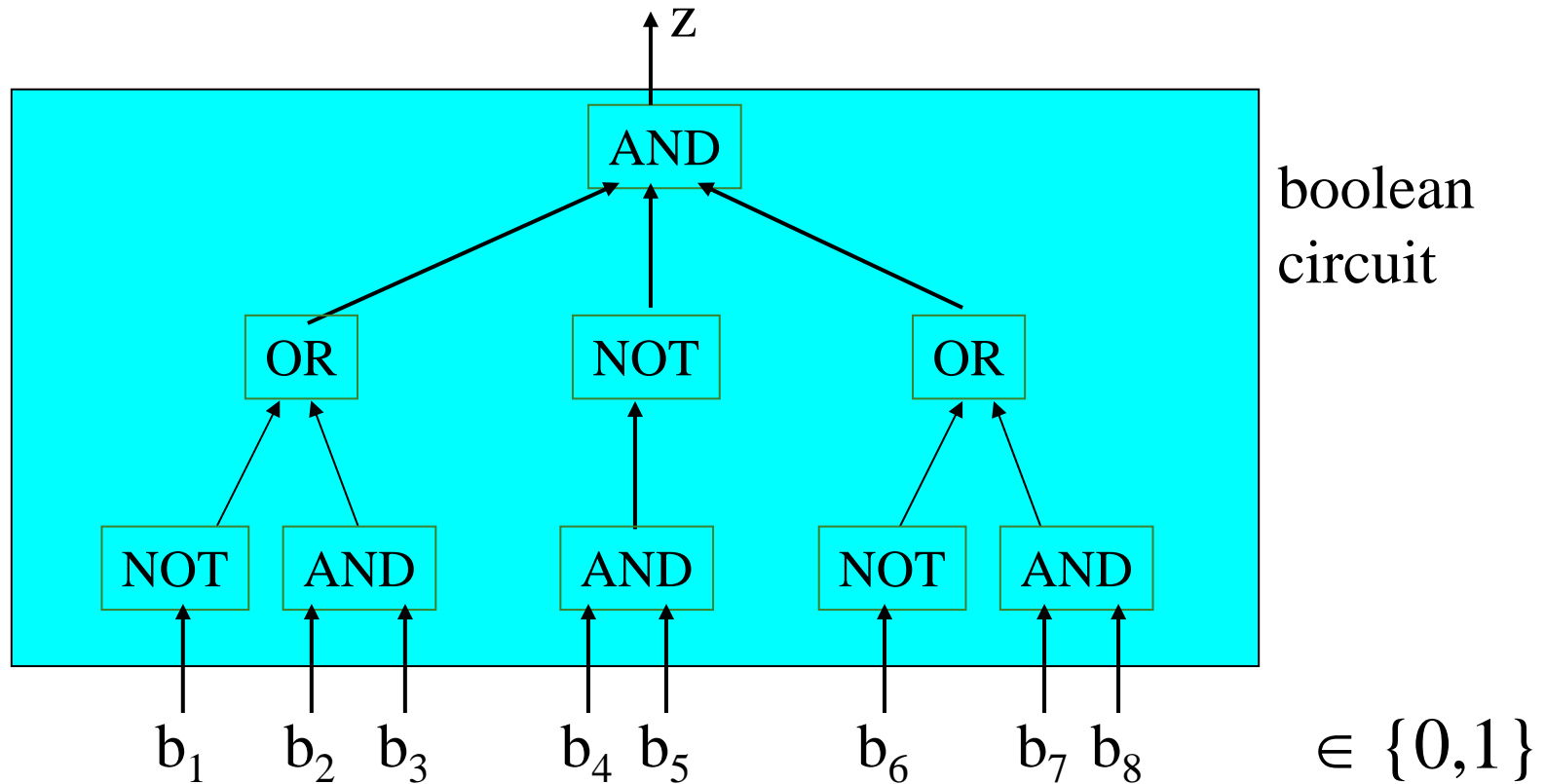
3. $D(\text{SK}, E(w_{i,j,k}))$

Total communication: $O(n^{1/3})$

Non-Interactive

Zero Knowledge [GOS'05]

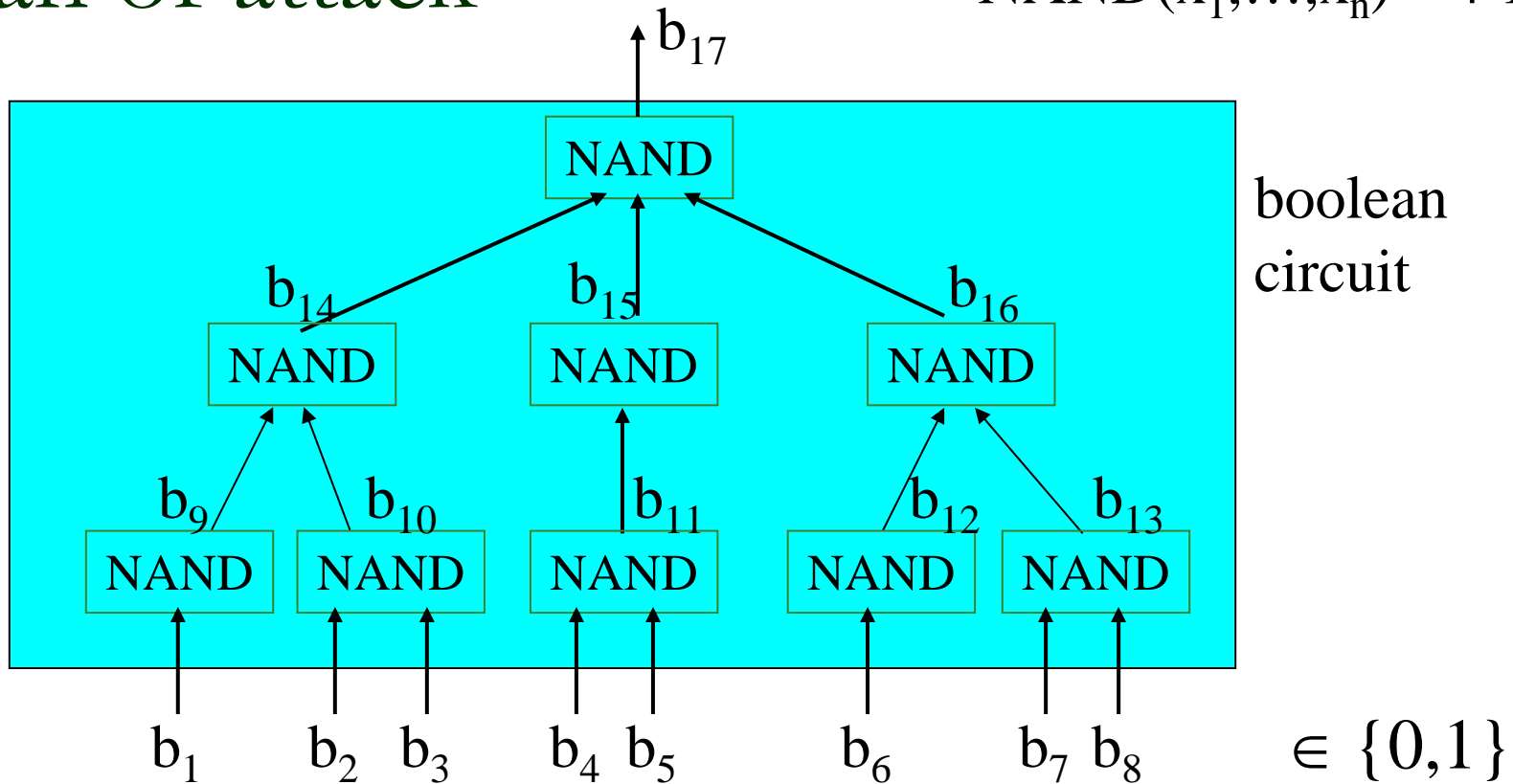
Goal: NIZK for circuit SAT



Goal: prover wants to convince verifier that circuit is satisfiable
in **zero knowledge** and **without interaction**

Plan of attack

$$\text{NAND}(x_1, \dots, x_n) = 1 - \prod x_i$$



Proof =

$\text{com}(b_1), \text{com}(b_2), \dots, \text{com}(b_m)$ and

for all gates (i,j,k) proof that:

$$b_i, b_j, b_k \in \{0,1\} \quad \text{and} \quad b_k = b_i \text{ NAND } b_j$$

Composite order commitments

- Common Random String: (G, g, g_p) , $|G|=N=pq$

- com(m): $r \leftarrow Z_N$, output $C \leftarrow g^m \cdot (g_p)^r$

note: $\text{com}(m_1) \cdot \text{com}(m_2)$ is commitment for (m_1+m_2)

- Fact: $z = x \text{ NAND } y \iff x, y, z, x+y+2(z-1) \in \{0,1\}$

- For a $C \in G$ we need a (w.i.) proof for the statement:

" $C = \text{com}(0)$ or $C = \text{com}(1)$ "

- Then for each gate (i,j,k) generate proof for:

$\text{com}(b_i)$, $\text{com}(b_j)$, $\text{com}(b_k)$, and

$\text{com}(b_i) \cdot \text{com}(b_j) \cdot [\text{com}(b_k) / \text{com}(1)]^2$

GOS (W.I.) Proof

- Common Random String: (G, g, g_p) , $|G|=N=pq$
- Let $C = g^m \cdot (g_p)^r$

$$\text{IF: } C = g \cdot (g_p)^r \quad \text{or} \quad C = (g_p)^r \quad (*)$$

$$\text{THEN: } L = e(C, Cg^{-1}) = e(g_p, \cdot) \in (G_T)^q$$

$$\forall m,r: e(C, Cg^{-1}) = e(\mathbf{g_p}, \underbrace{g^{2m-1} \cdot (g_p)^r}_{\text{(order p)}})$$

-
- Proof that (*) is true: $\pi = \mathbf{g^{2m-1} \cdot (g_p)^r} \in G$
 - To verify proof test if: $e(C, Cg^{-1}) \stackrel{?}{=} e(\mathbf{g_p}, \pi)$

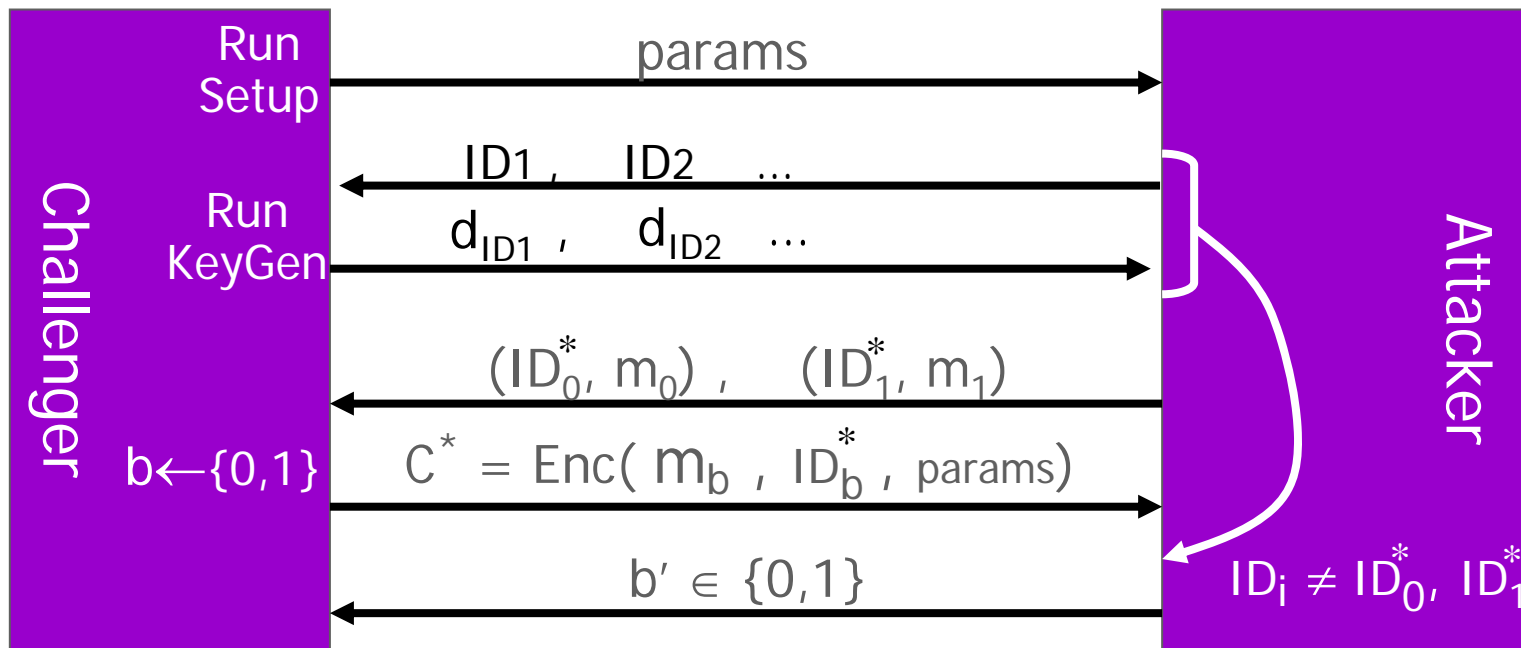
Why is the SAT proof Zero Knowledge?

- Common Random String: (G, g, g_p) , $|G|=N=pq$
 - Basic idea:
 - Simulator uses (G, g, g^s) as CRS
 - Indistinguishable by subgroup assumption
 - Commitment $C = g^m \cdot (g^s)^r$ contains no info on m
-
- Summary:
 - NIZK proof size: $O(|\# \text{ gates}| \cdot \lambda)$
 - CRS size: $O(\lambda)$

Anonymous IBE

Anonymous IBE [BDHP'04, AB...04]

- Ciphertext C should reveal no information about ID



- Secure if $Adv_A = |Pr[b=b'] - \frac{1}{2}|$ is negligible
- Anon-IBE is easy to construct in R.O. model

IBE system (selectively) secure without R.O. [BB'04]

- Setup: $\text{params} \leftarrow (w, u=g^x, v, h) \in G$; $\text{MK} \leftarrow v^x$
- KeyGen (ID, MK): given pub-key $\text{ID} \in \{1, \dots, q\}$ do:
 $r \leftarrow \{1, \dots, q-1\}$; $d_{\text{ID}} \leftarrow (\text{MK} \cdot (u^{\text{ID}} h)^r , w^r)$
- Encrypt (m, ID, (w,u,v,h)):
 $s \leftarrow \{1, \dots, q-1\}$; $C \leftarrow (m \cdot e(u, v)^s , w^s , (u^{\text{ID}} h)^s)$
- Decrypt (C, d_{ID}): details not important here

... but not anonymous

$$C = \left(m \cdot e(u, v)^s, \overset{B_1}{w^s}, \overset{B_2}{(u^{\text{ID}} \cdot h)^s} \right)$$

Note: $e(B_1, u^{\text{ID}} \cdot h) = e(w, B_2)$

$$\begin{aligned} &= e(w, u^{\text{ID}} \cdot h)^s \end{aligned}$$

$(w, u^{\text{ID}} \cdot h, B_1, B_2)$ form a DDH tuple

\Rightarrow Anyone can test if C is for ID_1 or ID_2

Composite order groups to the rescue ...

- $G = G_p \times G_q$ composite order group. $w, u, h \in G_p$
 - params: blind w, u, h by G_q
$$W \leftarrow w \cdot R_w, \quad U \leftarrow u \cdot R_u, \quad H \leftarrow h \cdot R_h \quad \text{where } R_w, R_u, R_h \in G_q$$

- Encrypt ($m, \text{ID}, (W, U, v, H)$): $s \leftarrow Z_N, \quad Z_1, Z_2 \leftarrow G_q$
$$C \leftarrow [m \cdot e(U, v)^s, \quad W^s \cdot Z_1, \quad (U^{\text{ID}} H)^s \cdot Z_2]$$
- No change to KeyGen and Decrypt (using w, u, h)
 - Note: R and Z terms cancel in Decrypt

- Now attack fails:
$$(W, U^{\text{ID}} \cdot H, W^s \cdot Z, (U^{\text{ID}} H)^s \cdot Z) \quad \text{not a DDH tuple in } G$$

The full system [BW'07]

- ... But cannot prove the system secure.

- The full system: add y to d_{ID}

- KeyGen(ID, MK): $t_1, t_2 \leftarrow Z_N$

$$d_{ID} \leftarrow (MK \cdot (u^{ID} \cdot h)^{t_1} \cdot y^{t_2}, w^{t_1}, w^{t_2})$$

- CT: $(m \cdot e(U, v)^s, w^s \cdot z_1, (U^{ID} \cdot H)^s \cdot z_2, Y^s \cdot z_3)$

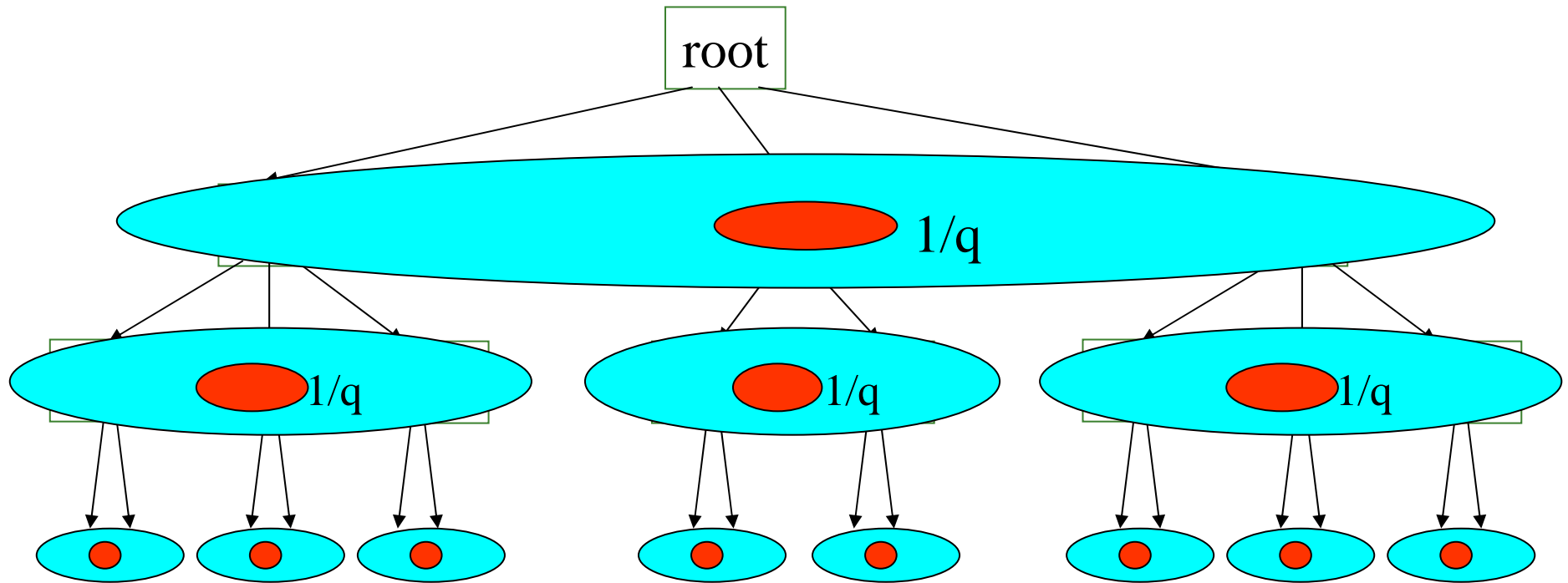
-
- Thm: (selective) Anon-IBE without R.O. assuming
 - Composite BDH assumption, and
 - Composite 3DH assumption

Open Problems

1. Tight HIBE

- Hierarchical-IBE [LH'02, GS'02, BB'04, BBS'04, BW'06]
 - In all known secure constructions, security proof degrades exponentially in **depth** of hierarchy
- Open Problem:
 - Find an HIBE construction where security proof degrades at most polynomially in hierarchy depth
 - Not known even in Random Oracle model

Problem with IBE/HIBE proof technique



Problem: $\Pr[\text{ID}^* = (I_1, I_2, \dots, I_d) \text{ is all "red"}] < 1/q^d$

Only works when depth $d = O(1)$

2. Tight VRF

- Verifiable Random Function (VRF):
 - $\text{Setup}(\lambda)$: output (PK, SK)
 - $\text{F}(\text{SK}, x)$: output y and proof π
 - $\text{verify}(x, y, \text{PK}, \pi)$: output yes/no
 - Security requirement: $\text{F}(\text{SK}, \cdot)$ must be a PRF
- Pairing-based constructions: [L'02, DY05]

$$\text{PK}=(g, g^\alpha) \quad , \quad \text{SK}=\alpha$$

$$\text{F}(\alpha, x) = e(g, g)^{1/(\alpha+x)} \quad ; \quad \pi = g^{1/(\alpha+x)}$$

but, security proofs take exponential time in $|x|$

Summary

- Bilinear groups of composite order:
 - Easy to construct using supersingular curves
 - Many applications:
 - hom. enc, PIR, anon-IBE, NIZK, group-sigs, ...

- Note: analogous constructions using the linear assumption in **prime** order groups:

$$g, u, v, g^x, u^y : v^{x+y} \approx g^z$$

- ... but constructions are by far more complex

- Many open problems remain in pairing based cryptography
 - Examples: Tight HIBE, Tight VRF



THE END