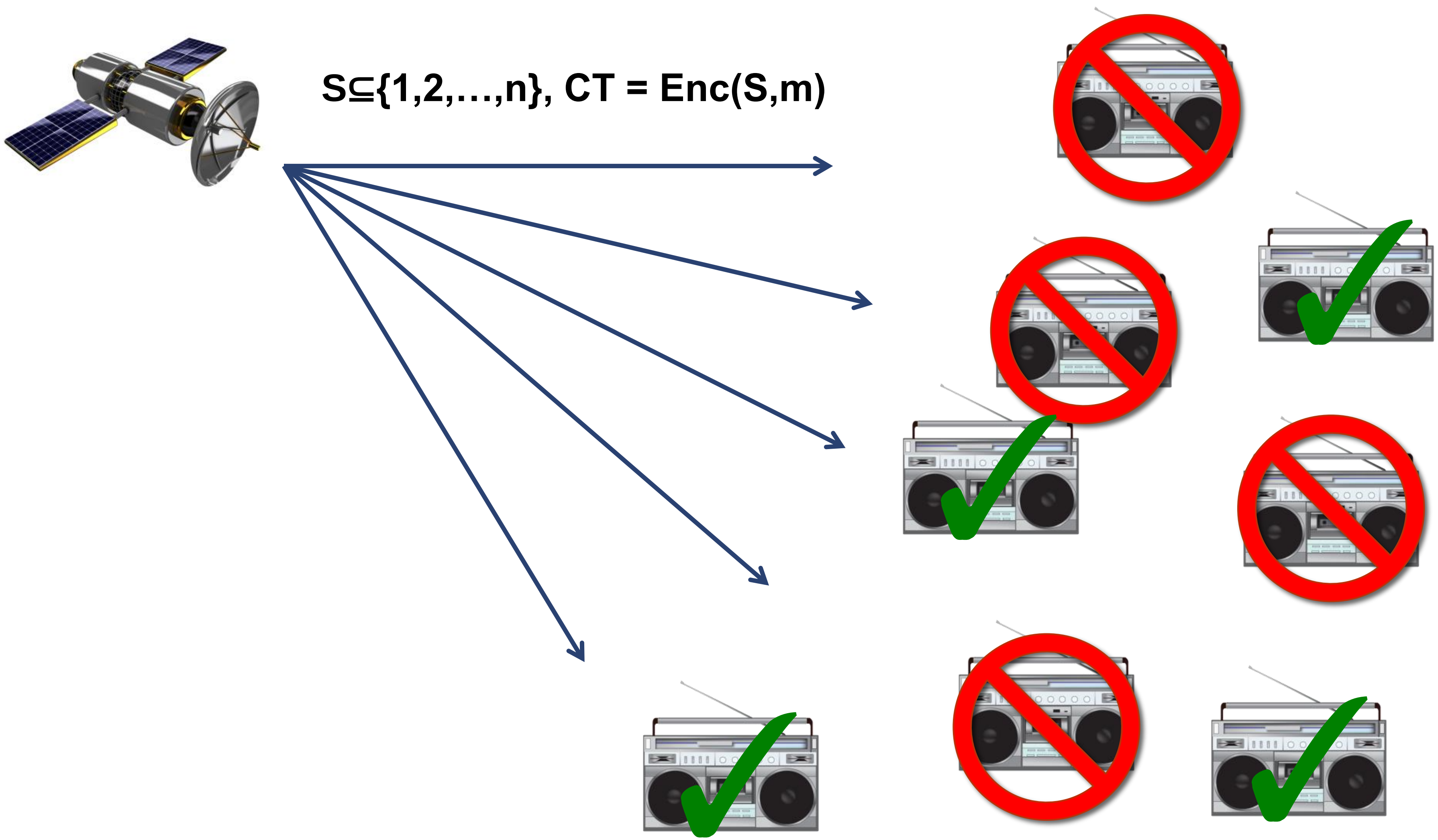
Low Overhead Broadcast Encryption from Multi-linear Maps

Dan Boneh — Stanford

Brent Waters — UT Austin

Mark Zhandry — Stanford

Broadcast Encryption



Broadcast Encryption

Trivial system: each user has secret/public key

Goal: smallest parameter sizes

n = # of users

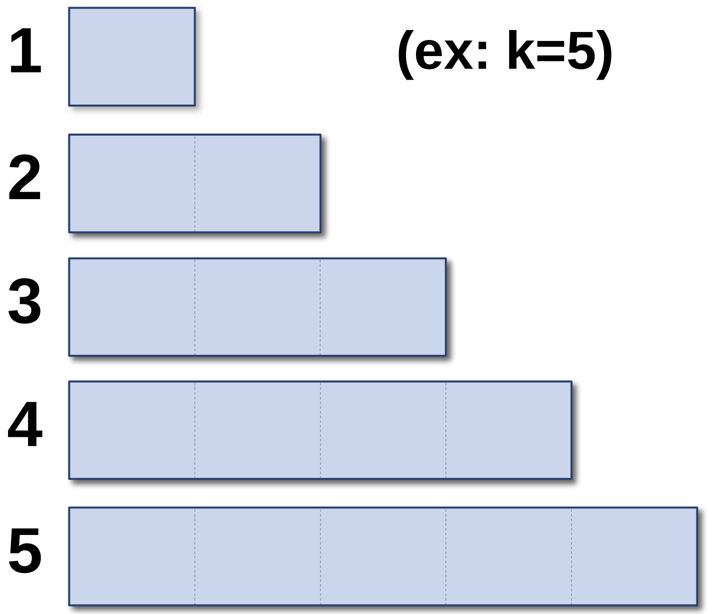
Scheme	|CT|	|SK|	|PP|, |BK|	PK?	Assumption
Trivial	$O(\|S\|)$	$O(1)$	$O(n)$	✔ □	PKE
BGW'05	$O(1)$	$O(1)$	$O(n)$	✔ □	BDHE
BGW'05	$O(\sqrt{n})$	$O(1)$	$O(\sqrt{n})$	✔ □	BDHE
BS'03+ GGH'13	$O(1)$	$n^{O(1)}$	$n^{O(1)}$	✗	MDHI
BZ'13	$O(1)$	$O(1)$	$n^{O(1)}$	✔ □	iO

Multilinear Maps (aka Graded Encodings)

k Levels:

Encoding ring elements:

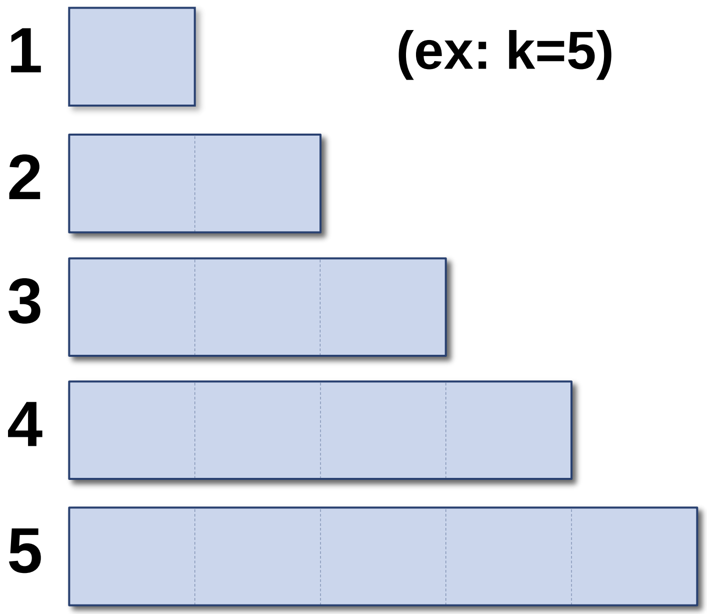
(ex: k=5)



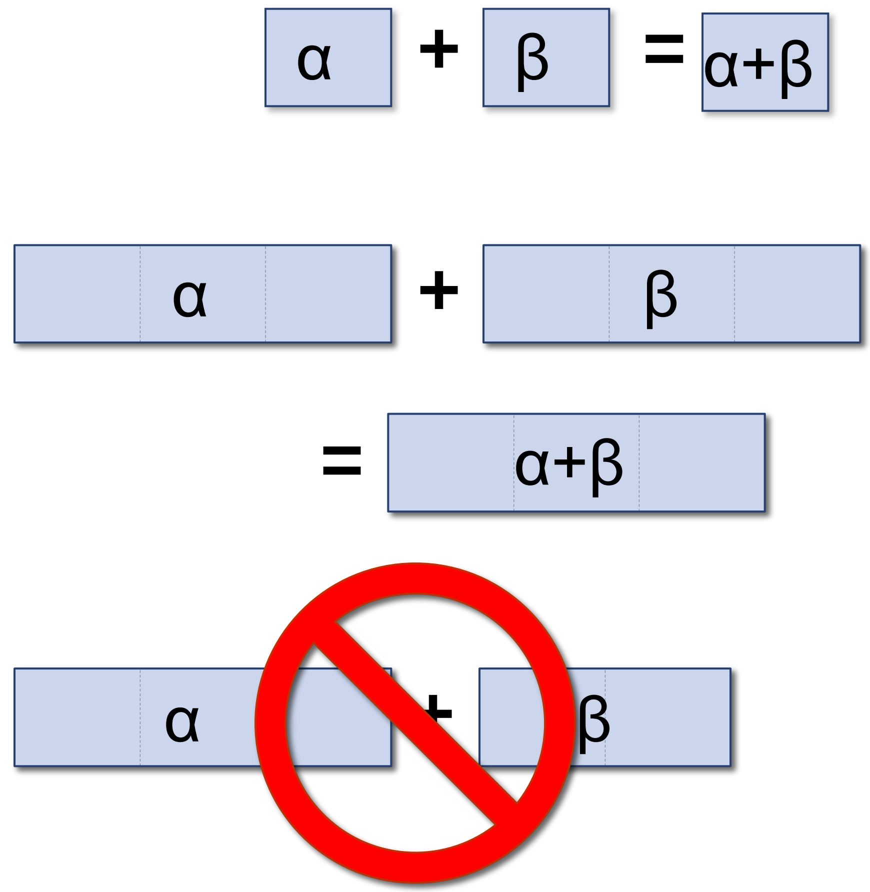
Multilinear Maps (aka Graded Encodings)

k Levels:

(ex: k=5)



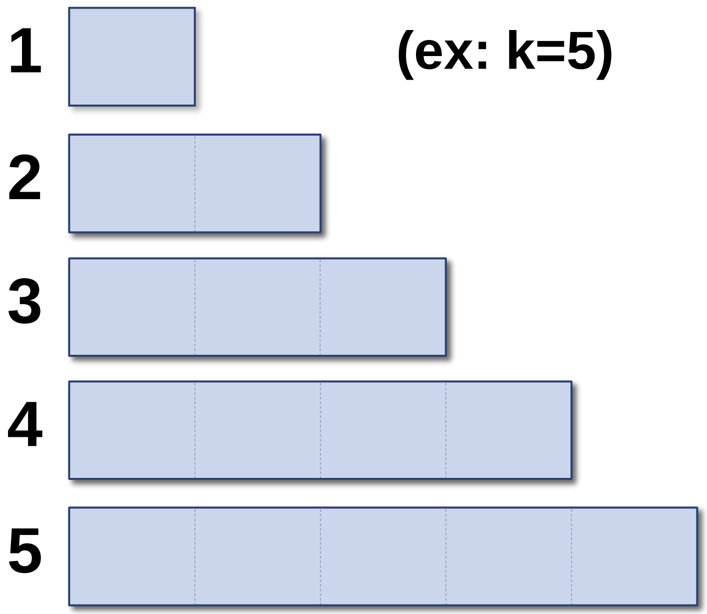
Add within levels:



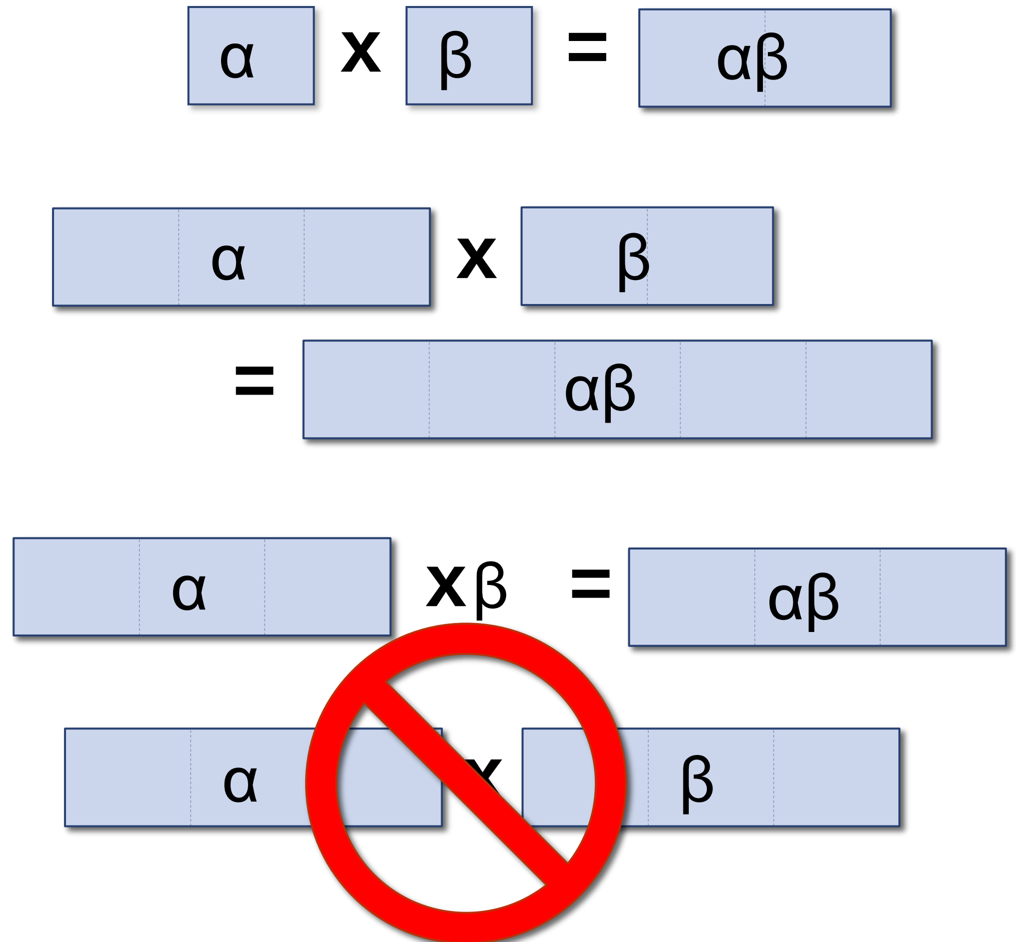
Multilinear Maps (aka Graded Encodings)

k Levels:

(ex: k=5)



Multiply up to level **k**



Problem with Using Multilinear Maps

BS'03 (secret key) solution:

CT overhead: **0** (public key variant: **1** group element)

SK: **1** group element

BK: Map description, some scalars

Multilinearity: **k = n**

Problem with GGH'13, CLT'13: **|group element| = Ω(k)**

|map description| = Ω(k)

⇒ **|SK| = Ω(k), |PP| = Ω(k)** (**|CT| = Ω(k)** for public key variant)

To use multilinear maps for BE, need **k << n**

Starting Point: BGW'05 **(k = 2)**

User set: **$[g-1] = \{1,2,\ldots,g-1\}$**

Setup:

$\alpha,\beta \leftarrow R$

"Gap" at **g**

PP: α | α^2 | α^3 | … α^{g-1} | ◯ | α^{g+1} | α^{g+2} | … α^{2g-2} | β

sk_i: $\beta\alpha^i$

For any **$S \subseteq [g-1]$, $i \in S$**, define

$$u_S = \Sigma_{j\in S}\alpha^{g-j} \quad u_S^{(i)} = \Sigma_{j\in S\setminus\{i\}}\alpha^{g+i-j}$$

Property: **$u_S\alpha^i - u_S^{(i)} = \alpha^g$**

Given **PP**, can compute: u_S $u_S^{(i)}$

Starting Point: BGW'05 **(k = 2)**

Enc(S):

t ← R

CT: t , $t \times (\beta + u_S) = t(\beta+u_S)$

K_{enc}: $t \times \alpha^{g-1} \times \alpha = t\alpha^g$

Dec(S, sk_i = $\beta\alpha^i$ t $t(\beta+u_S)$

$$K_{enc} = \alpha^i \times t(\beta+u_S) - (\beta\alpha^i + u_S^{(i)}) \times t = t\alpha^g$$

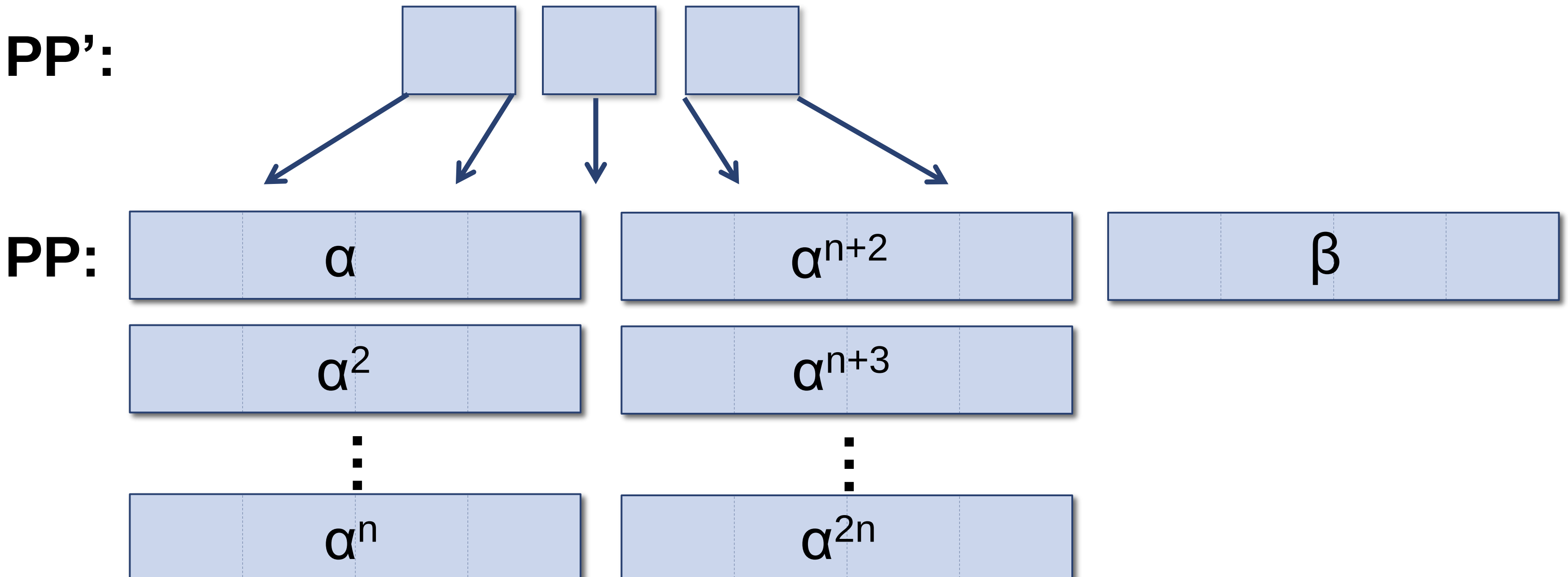
Note: if no gap at **g** anyone can decrypt: $K_{enc} = t \times \alpha^g$

New Idea: Use Map to Generate PP

BGW'05: Too many components in **PP**

Idea: Put BGW'05 in intermediate levels of multilinear map

Use map to generate **PP** from small level **1** set **PP'**



What elements should **PP'** consist of?

Abstract Construction

ID: User space

CT, sk: Level **m** and **h** encodings of **(m+h)**-linear map

PP': level-1 encodings of $\boldsymbol{\alpha}^j$ for $\mathbf{j \in T}$ (and $\boldsymbol{\beta}$ at level **m**)

PP': $\{ \alpha^j \}_{j \in T}$, β ← Level **m**

CT: t , $t(\beta + u_S)$ **sk_i:** $\beta\alpha^i$

Level **h**

Need to be able to compute the following from **PP**:

- For enc: u_S
- For dec: $u_S^{(i)}$ α^i

No security if able to compute: α^g

Needed Properties

s-span(T) = sums of **≤s** (possibly repeating) elements of **T**

Need sets **T,ID,** integers **g,h,m** such that:

- **$j \in$ h-span(T) $\forall j \in$ ID** (for $\boldsymbol{\alpha}^j$ at level h)
- **$g - i \in$ m-span(T) $\forall i \in$ ID** (for $\mathbf{u}_S$ at level m)
- **$g + j - i \in$ m-span(T) $\forall i,j \in$ ID, $i \neq j$** (for $\mathbf{u}_S^{(j)}$ at level m)
- **$g \in$(m+h)-span(T)** (for $\boldsymbol{\alpha}^g$ at level m+h)
- **$g \notin$ m-span(T)** (to block trivial attack)

Goal: Maximize **|ID|** (# users), Minimize **|T|** (# **PP**), **h+m** (# levels)

Simple **T** (for nice assumption)

Generalization of BGW'05:

m = h = 1 ID = [g-1] (n = g-1) T = {1,…,g-1,g+1,…,2g-2}

Our New Scheme

$T = \{ 1, 2, \ldots, 2^{m+1} \}$, $g = 2^{m+1} - 1$

$ID = \{ i<g : Hamming(i) = h \}$ for **$1 \leq h \leq m$**

- $j \in h\text{-span}(T)\ \forall j \in ID$ ✓
- $g - i \in m\text{-span}(T)\ \forall i \in ID$ ✓
- $g + j - i \in m\text{-span}(T)\ \forall i,j \in ID,\ i \neq j$ ✓
- $g \in (m+h)\text{-span}(T)$ ✓
- $g \notin m\text{-span}(T)$ ✓

Multilinear Diffie-Hellman Exponent Assumption

Given: α^1 α^2 α^4 … $\alpha^{2^{m+1}}$

t ← Level **h**

$t\alpha^{2^{m+1}-1}$ ← Level **m+h**

≈

r

Theorem: (m,h)-MDHE ⇒ static security

Parameter Sizes

Number of users: $\mathbf{n} = \binom{m+1}{h}$

For best **n**, set **m≅log n + ½ loglog n, h≅m/2**

- Total multilinearity: **O(log n)**
- Size of group elements, map parameters: **polylog(n)**
- Size of all params: **polylog(n)**

Since all params polylog, can set $\mathbf{n=2^{\lambda}}$

⇒ Identity based scheme

Setting of **m,h** to minimize **m+h**

n	**m**	**h**	**k=m+h**
2^4	5	3	8
2^8	10	4	14
2^{16}	18	8	26
2^{32}	35	15	50
2^{64}	68	29	97
2^{128}	136	53	189
2^{256}	270	104	374
2^{512}	533	211	744

Conclusion and Open Problems

Broadcast scheme with polylog parameters from M-maps

(two other variants with various trade-offs)

Open questions:

- Adaptive security
- Low overhead traitor tracing from **O(log |n|)**-linear maps
- Circuit ABE from **O(log |C|)**-linear maps
- Other applications of M-maps with low multilinearity