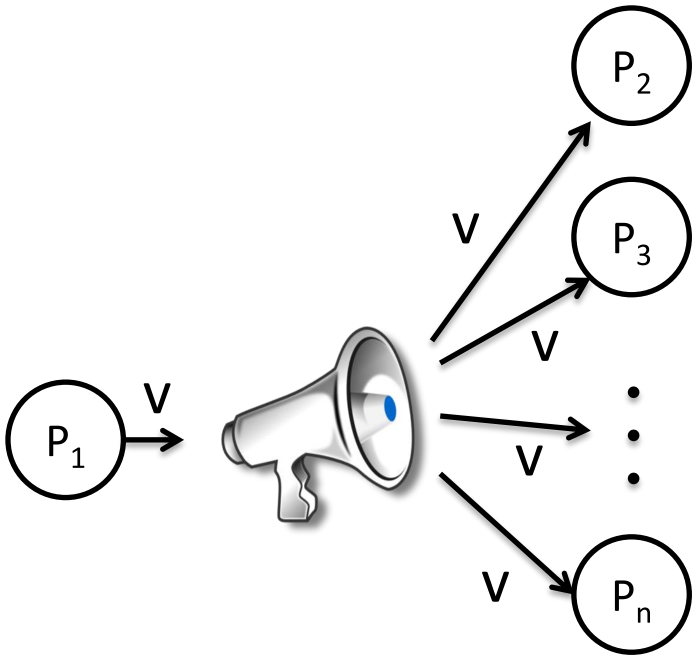
Multi-Valued Byzantine Broadcast: the t < n Case

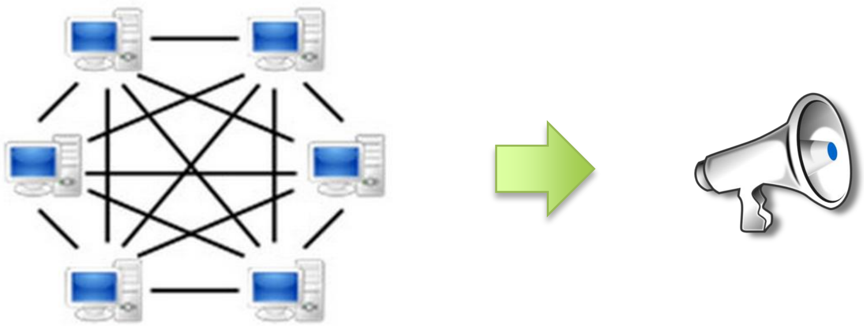
Martin Hirt, **Pavel Raykov**
ETH Zurich

Asiacrypt 2014

Byzantine Broadcast

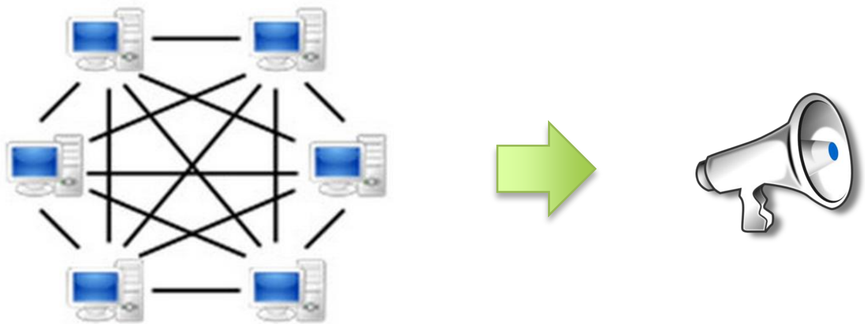


Broadcast Protocols



- For $t < n/3$ [PSL80,BGP92]
- For $t < n$ (assuming setup) [DS83, PW96]

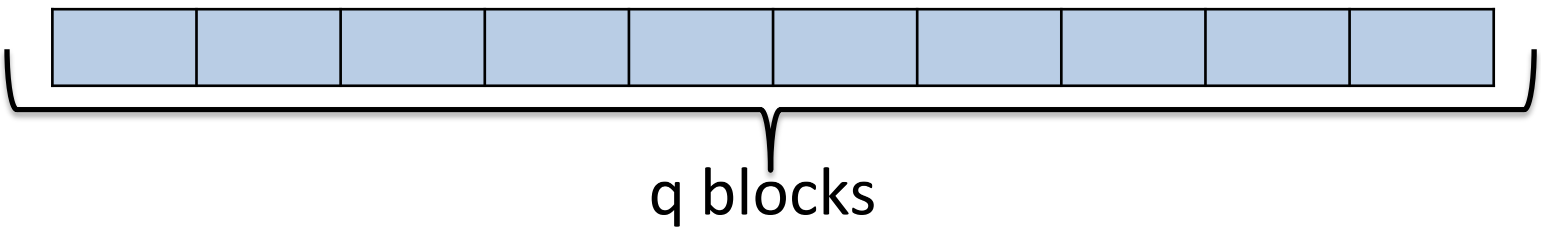
Broadcasting L Bits Efficiently



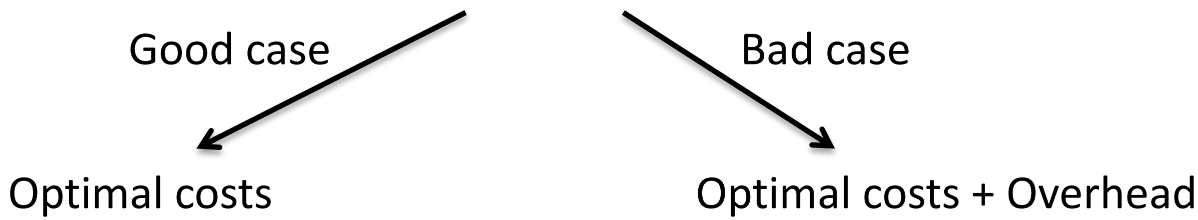
- Seminal protocols communicate $\Omega(Ln^2)$
- Optimal $O(Ln)$
- Solution – special-purpose multi-valued protocols:
  - Optimal for $t < n/3$ [LV11,Pat11]
  - Optimal for $t < n/2$ [FH06]
  - Optimal for $t < n$ [This work]

Overview of Our Protocol

1. Split message into many blocks:



2. Introduce optimistic block broadcast:

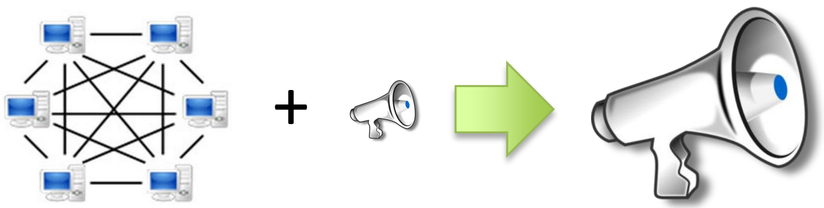


3. Broadcast message block by block optimistically s.t. bad cases are limited.

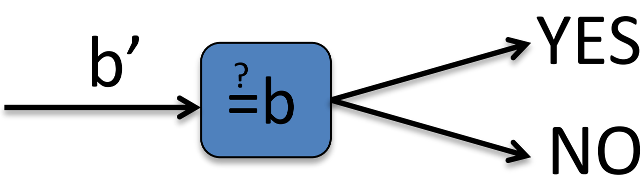
4. Fine-tune q to make bad case costs small.

Optimistic Broadcast of Block b

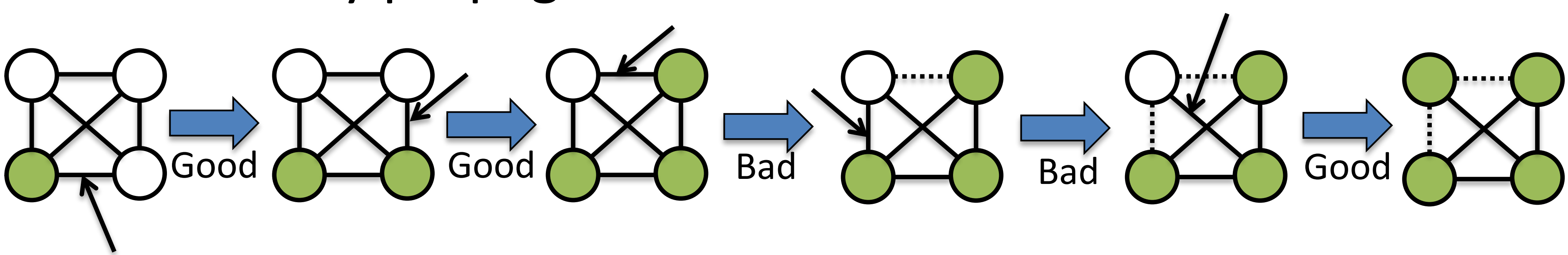
1. Assume we can broadcast few bits



2. The sender broadcasts h(b)

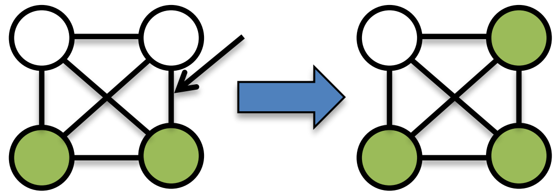


3. Iteratively propagate b



Computing Costs

1. One iteration of block's b propagation costs ≈ $|b| = \dfrac{L}{q}$



2. Broadcasting the i^{th} block optimistically:

Good case [0 iterations are bad] $\quad n \cdot |b|$

Bad case [d_i iterations are bad] $\quad (n + d_i) \cdot |b|$

3. Broadcasting block by block (q blocks):

$$\sum_{i=1}^{q} (n + d_i) \cdot |b| = \sum_{i=1}^{q} n \cdot |b| + \sum_{i=1}^{q} d_i \cdot |b| \leq Ln + n^2 \frac{L}{q}$$

4. Fine-tuning q: Setting q to n achieves O(Ln).

Review of the Protocol

1. Split L-bit message in q blocks.
2. Optimistic block broadcast: good and bad cases.
3. Broadcast message block by block s.t. bad cases are limited.
4. Fine-tune q s.t. bad costs are small.

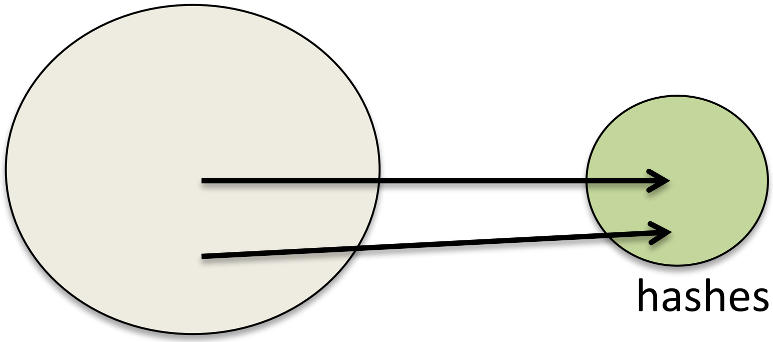
Achieve optimal communication complexity

Cryptographic security

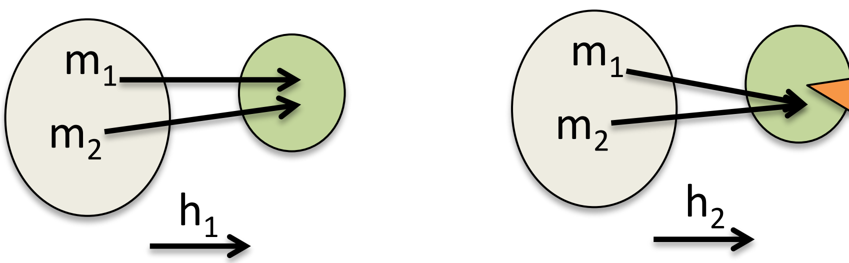
Can we get IT security?
Yes, but...

Universal Hashing

- Traditional hashing



- ε-Universal hashing family h_1, … h_t

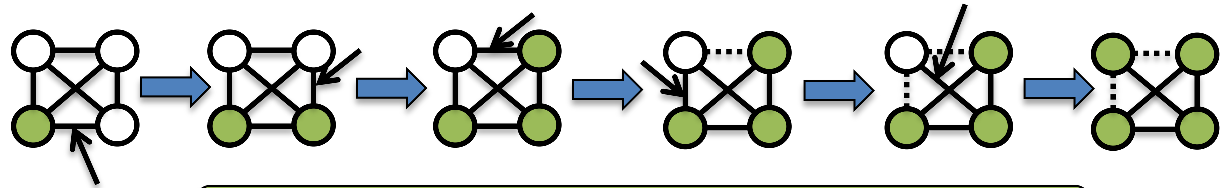


Fact: we know how to construct "good" universal hashing families

Security: For any fixed m_1,m_2 fraction of … ε.

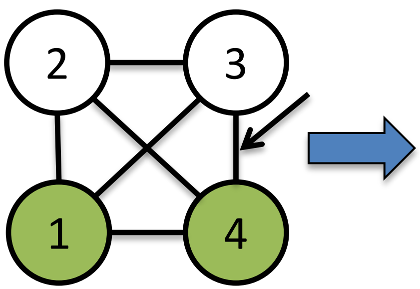
IT Optimistic Broadcast of Block b

With crypto hash:



Invariant – green have the same value.

With universal hash:



1. Choose a non-conflicting edge (3-4).
2. The candidate (3) receives b' from the green (4)
3. The candidate generates random key r and broadcasts r, $y_3=h_r(b')$.
4. Each of the green (1,4) broadcasts $y_i=h_r(b)$.

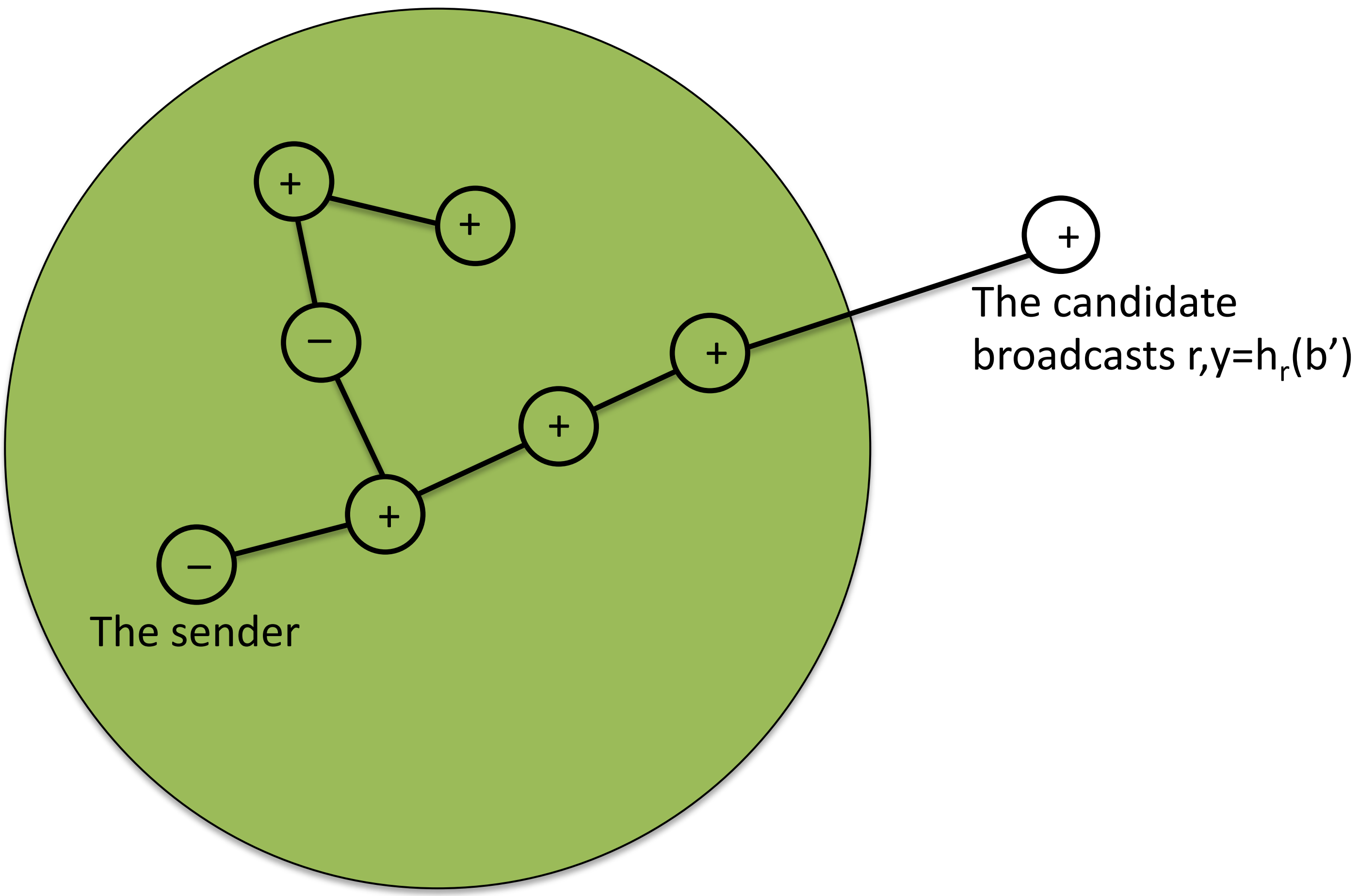
Good case

1. Everyone has the same value ($y_1=y_4=y_3$).
2. Add the candidate to green.

Bad case

1. Extract a conflict.
2. Restart.

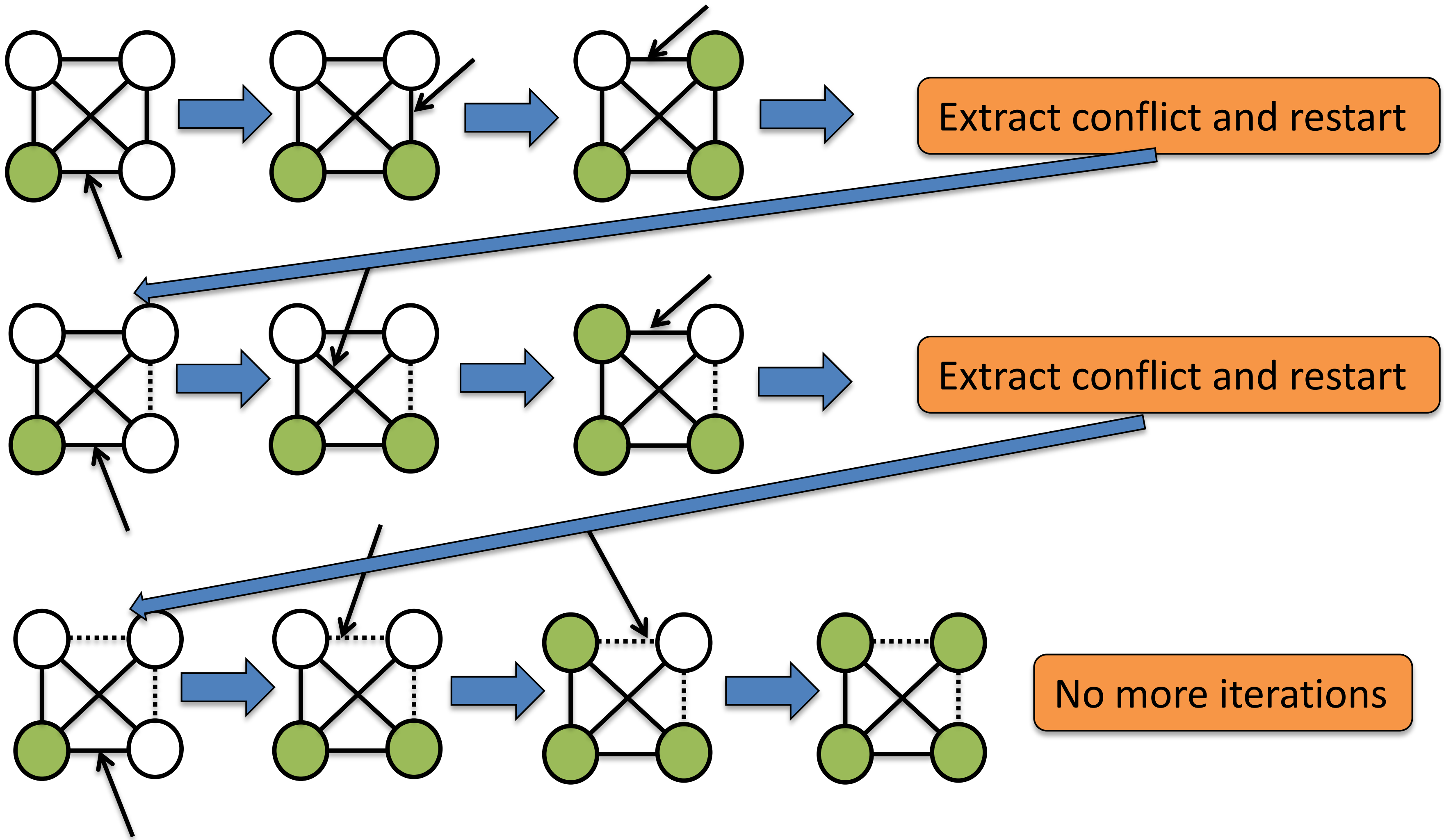
Extracting the Conflict



Lemma 1: All players form a "learning" tree with the sender in its root.

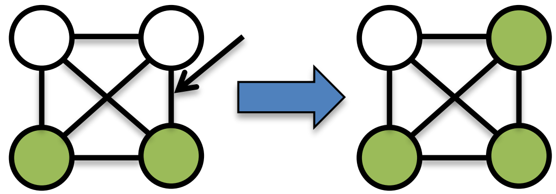
Lemma 2: If >0 players have "+" and >0 players have "–", there is a (+,-) edge.

An Example of IT block Propagation



Computing Costs (IT Case)

1. One iteration of block's b propagation costs ≈ $|b| = \frac{L}{q}$



2. Broadcasting the ith block optimistically:

Good case [0 iterations are bad]

$$n \cdot |b|$$

Bad case [d_i iterations are bad]

$$(n + \underbrace{d_i}_{\cdot n}) \cdot |b|$$

3. Broadcasting block by block (q blocks):

$$\sum_{i=1}^{q} (n + \underbrace{d_i}_{\cdot n}) \cdot |b| = \sum_{i=1}^{q} n \cdot |b| + \sum_{i=1}^{q} \underbrace{d_i}_{\cdot n} \cdot |b| \leq Ln + n^{3} \frac{L}{q}$$

4. Fine-tuning q: Setting q to n^{2} achieves O(Ln).

Comparing Costs

- Crypto case

$\Omega(Ln^2 + n^3\kappa)$	[DS83]
$O(Ln + n^5\kappa)$	Our Crypto construction

- IT case

$\Omega(Ln^2 + n^6\kappa)$	[PW96]
$O(Ln + n^{10}\kappa)$	Our IT construction

Conclusions

- The first communication-optimal multi-valued broadcast for $t < n$.
- Future research:
  - better concrete efficiency
  - tolerating mobile adversary