On the Intrinsic Complexity of Broadcast

Martin Hirt

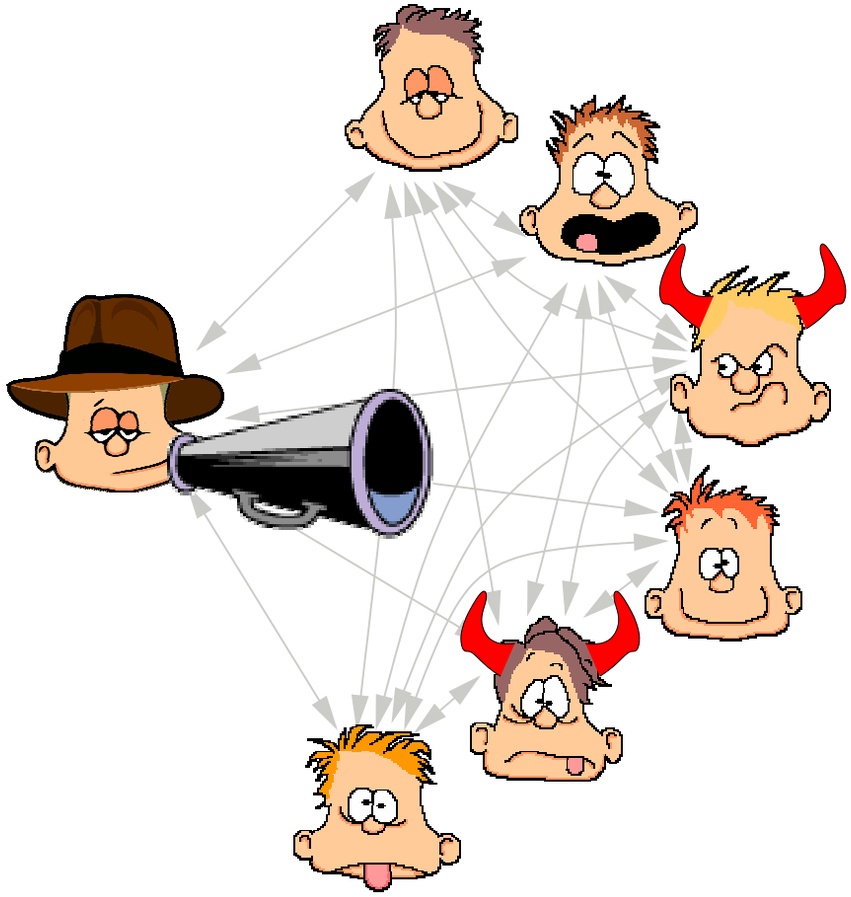
joint work with **Ueli Maurer** and **Pavel Raykov**

ETH Zurich

Theory and Practice of MPC, Aarhus, May 2014

The Setting

- A sender, and n recipients (up to t dishonest)
- Bilateral channels (available for free)
- Goal: broadcast **arbitrary long message**



Broadcast:

Consistency: All recipients get the same value

Validity: If the sender is honest, this is his value

Approaches

How to achieve Broadcast?

- $t < n/3$: use your favorite protocol, e.g. [LSP82,BGP89,CW89,. . .]
- $t \geq n/3$: impossible [LSP82]

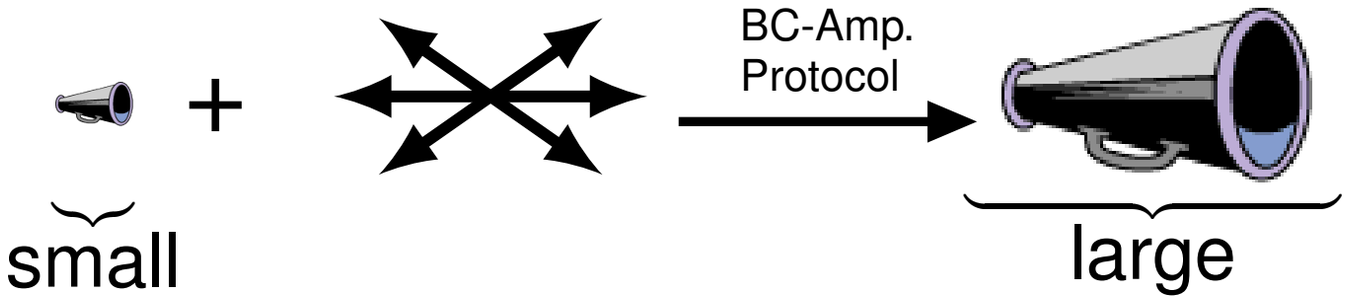
How to achieve Broadcast anyway? ($t \geq n/3$)

- Assume trusted party  that distributes PKI **(consistently!)**, then use [DS82,PW96,. . .]
- Assume "small" broadcast primitive 

Broadcast Amplification

Broadcast Amplification

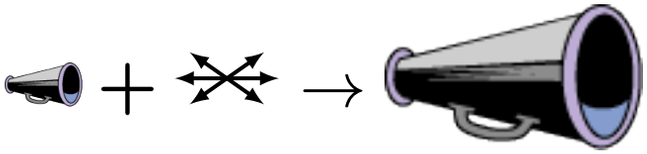
What it is



Note

- Only interesting for $t \geq n/3$

Goals

1. Find amplification protocols: 
2. Proof lower bounds for size of 

Intrinsic Complexity

Def: d-broadcast = broadcast for domain size d (i.e., $\log d$ bits)

The Intrinsic Complexity of Broadcast

$\phi_n(d)$ = minimal domain size of the available broadcast primitive to achieve d-broadcast among n parties.

Note: $\phi_n(d) \leq d$

We totally ignore the size of 

Outline

On the Intrinsic Complexity of Broadcast

- Warm-Up
- The $n = 3$ Case
- The $n \geq 4$ Case
- Conclusions

Warm-Up: Cryptographic Security

Model: cryptographic security, $t < n$

Protocol

1. $\forall P_i$: select random SK/PK
2. $\forall P_i$: broadcast PK (using available 📣)
3. invoke [DS82] to broadcast message (using 🔀)

Analysis

- $n\kappa$ bits through 📣 (+ some 🔀, we don't care)

Can we do better?

smaller 📣

statistical / perfect security

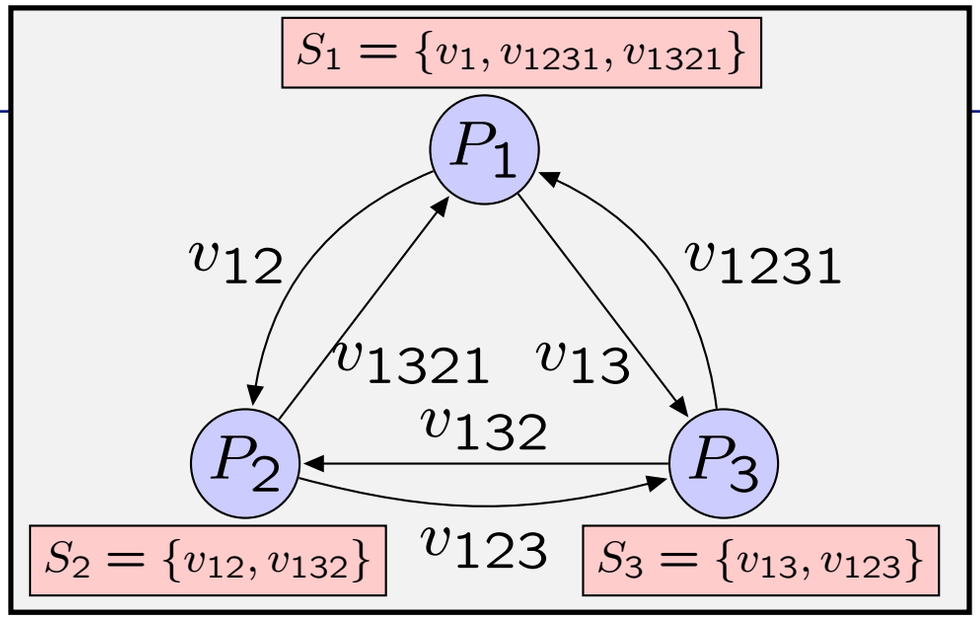
Yes, we can!

Outline

On the Intrinsic Complexity of Broadcast

- Warm-Up
- The $n = 3$ Case
- The $n \geq 4$ Case
- Conclusions

The $n = 3$ Case [1/5]



Protocol ($n = 3$)

0. Sender P_1 holds v_1
1. $P_1 \xrightarrow{v_{12}} P_2 \xrightarrow{v_{123}} P_3 \xrightarrow{v_{1231}} P_1$
2. $P_1 \xrightarrow{v_{13}} P_3 \xrightarrow{v_{132}} P_2 \xrightarrow{v_{1321}} P_1$
3. P_1: hint h supports v_1, excludes v_{1231} and v_{1321}, broadcast using 📣
4. P_2/P_3: accept value in S_2/S_3 supported by h

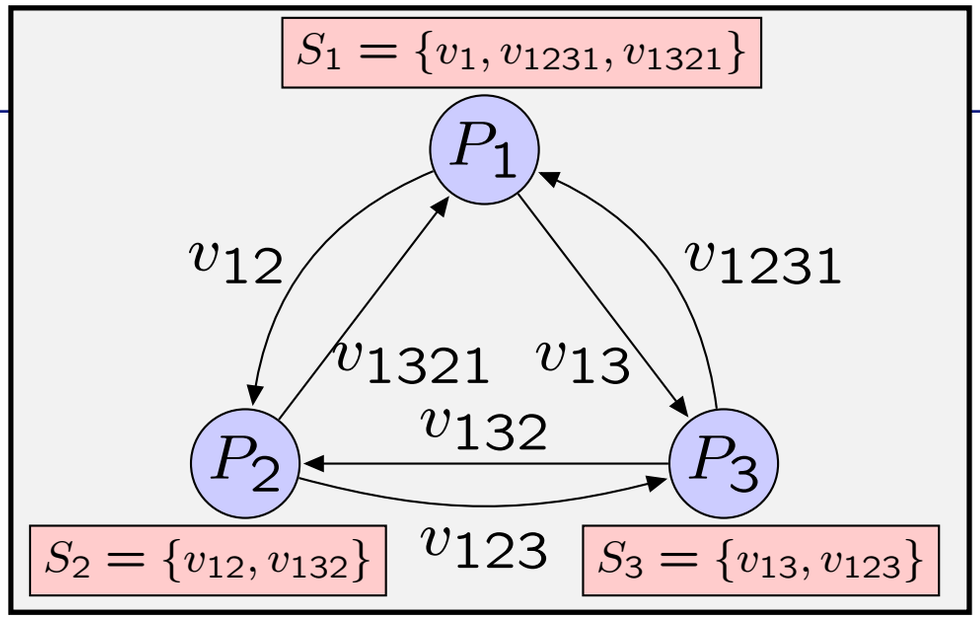
Computing the Hint

v_1	$=$	a_1	a_2	a_3	a_4	a_5	a_6	a_7	a_8
v_{1231}	$=$	b_1	b_2	b_3	b_4	b_5	b_6	b_7	b_8
v_{1321}	$=$	c_1	c_2	c_3	c_4	c_5	c_6	c_7	c_8

$i = 3, j = 7,$

$\boldsymbol{h = (i, a_i, j, a_j)}$

The $n = 3$ Case [2/5]



Protocol ($n = 3$)

0. Sender P_1 holds v_1
1. $P_1 \xrightarrow{v_{12}} P_2 \xrightarrow{v_{123}} P_3 \xrightarrow{v_{1231}} P_1$
2. $P_1 \xrightarrow{v_{13}} P_3 \xrightarrow{v_{132}} P_2 \xrightarrow{v_{1321}} P_1$
3. P_1: hint h supports v_1, excludes v_{1231} and v_{1321}, broadcast using 📣
4. P_2/P_3: accept value in S_2/S_3 supported by h

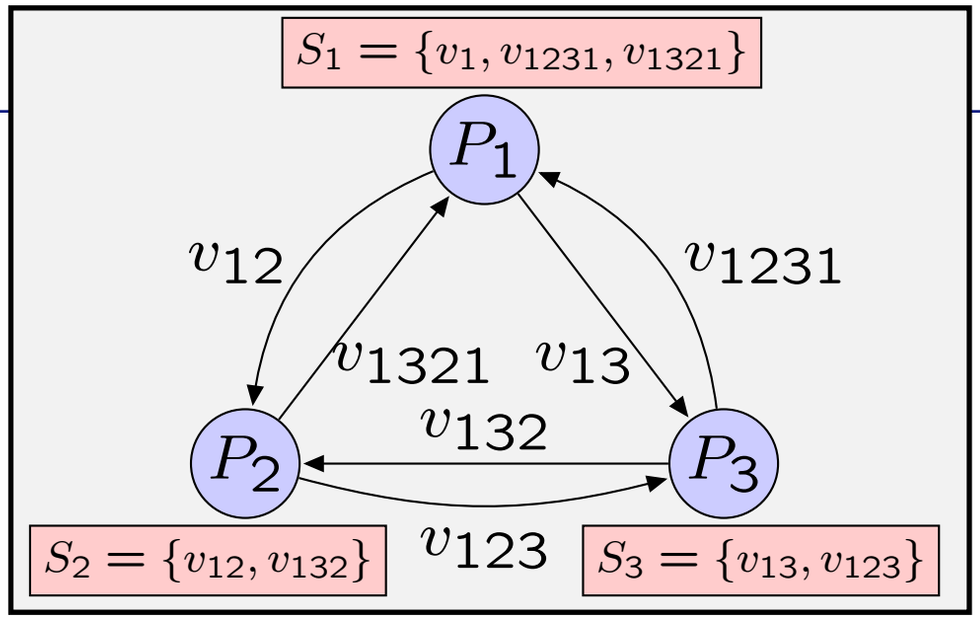
Analysis

- Validity: P_1 and P_i honest $\rightarrow v_1 \in S_i \subseteq S_1 \rightarrow P_i$ decides on v_1
- Consistency: P_2 and P_3 honest $\rightarrow S_2 = S_3 \rightarrow$ decide the same
- Efficiency: $\ell' = 2 \log \ell + 2$

Example: 1 MB $\rightarrow$ 42 Bits

Can we do better?
Yes, use **Recursion**

The $n = 3$ Case [3/5]



Protocol ($n = 3$)

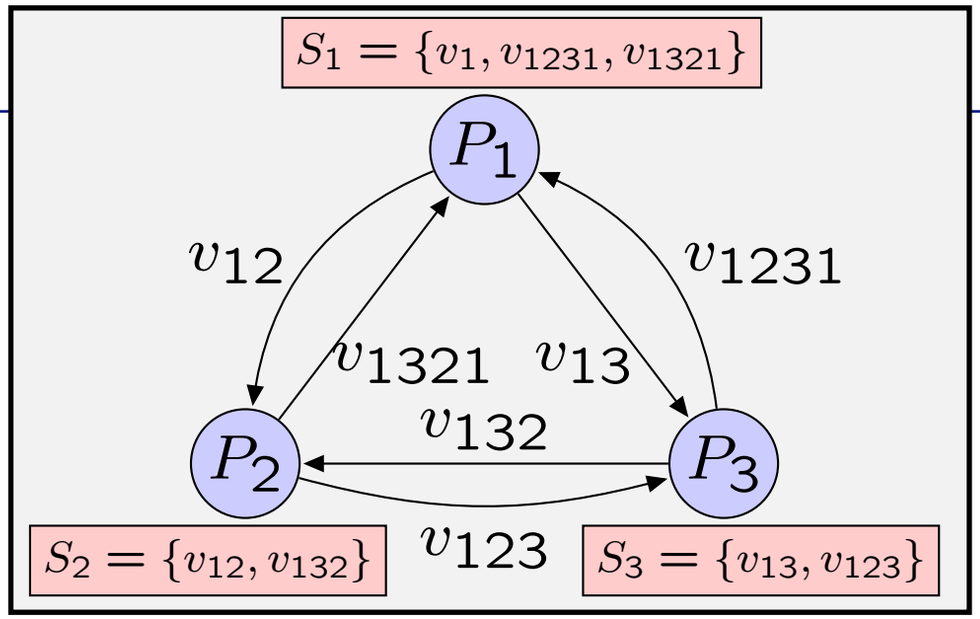
0. Sender P_1 holds v_1
1. $P_1 \xrightarrow{v_{12}} P_2 \xrightarrow{v_{123}} P_3 \xrightarrow{v_{1231}} P_1$
2. $P_1 \xrightarrow{v_{13}} P_3 \xrightarrow{v_{132}} P_2 \xrightarrow{v_{1321}} P_1$
3. P_1: hint h supports v_1, excludes v_{1231} and v_{1321}, broadcast using 📣
4. P_2/P_3: accept value in S_2/S_3 supported by h

Recursion

- Remember $\ell' = 2\log\ell + 2$
- Recursion: ℓ bits $\rightarrow 2\log\ell + 2$ bits
  $\rightarrow 2\log(2\log\ell + 2) + 2$ bits
  $\ldots$
  $\rightarrow 10$ bits
- I.e.: $\phi_3(\cdot) \leq 2^{10}$

Can we do better?
Yes, use **better Hint**

The $n = 3$ Case [4/5]



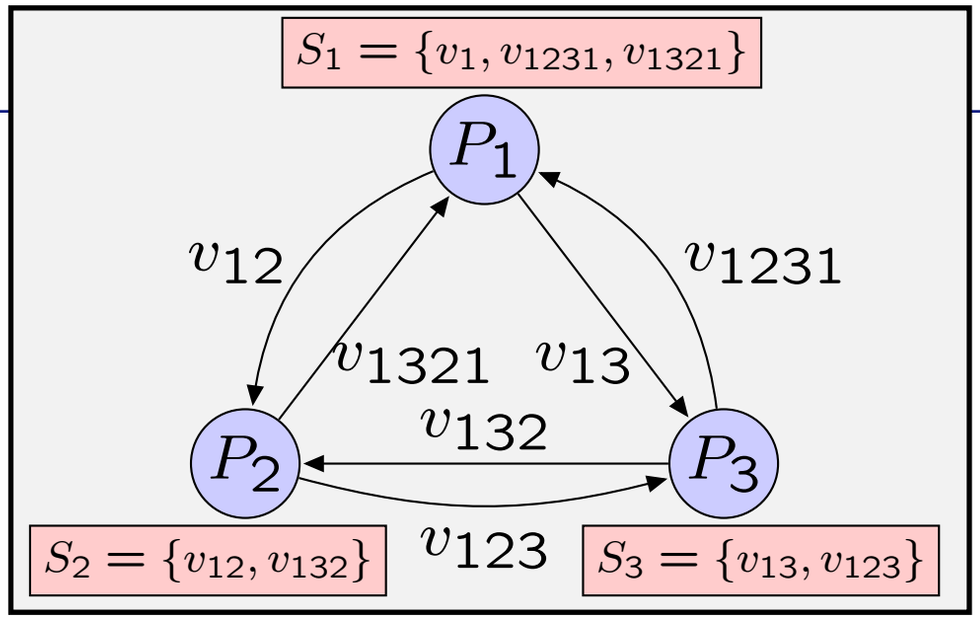
Protocol ($n = 3$)

0. Sender P_1 holds v_1
1. $P_1 \xrightarrow{v_{12}} P_2 \xrightarrow{v_{123}} P_3 \xrightarrow{v_{1231}} P_1$
2. $P_1 \xrightarrow{v_{13}} P_3 \xrightarrow{v_{132}} P_2 \xrightarrow{v_{1321}} P_1$
3. P_1: hint h supports v_1, excludes v_{1231} and v_{1321}, broadcast using 📣
4. P_2/P_3: accept value $\boxed{\begin{cases} h, & \text{if } h \in S_i \\ v_\star, & \text{otherwise} \end{cases}}$

"Better" Hints

- Domain D, i.e., $v_1 \in D$, with $|D| \geq 4$
- $D' := D \setminus \{v_\star\}$, where $v_\star =$ "largest value in D", $h \in D'$
- $h \leftarrow \begin{cases} v_1, & \text{if } v_1 \neq v_\star \\ v \in D' \setminus S_1, & \text{otherwise} \end{cases}$

The $n = 3$ Case [5/5]



Protocol ($n = 3$)

0. Sender P_1 holds v_1
1. $P_1 \xrightarrow{v_{12}} P_2 \xrightarrow{v_{123}} P_3 \xrightarrow{v_{1231}} P_1$
2. $P_1 \xrightarrow{v_{13}} P_3 \xrightarrow{v_{132}} P_2 \xrightarrow{v_{1321}} P_1$
3. P_1: hint h supports v_1, excludes v_{1231} and v_{1321}, broadcast using 📣
4. P_2/P_3: accept value $\begin{cases} h, & \text{if } h \in S_i \\ v_\star, & \text{otherwise} \end{cases}$

Analysis

- Validity: P_1 and P_i honest $\rightarrow v_1 \in S_i \subseteq S_1 \rightarrow P_i$ decides on v_1
- Consistency: P_2 and P_3 honest $\rightarrow S_2 = S_3 \rightarrow$ decide the same
- Efficiency: $|D'| = |D| - 1$
- Recursion: $\ldots |D^{(k)}| = 3$

Can we do better?
$\rightarrow$ **No!** $\phi_3(\cdot) = 3$

Outline

On the Intrinsic Complexity of Broadcast

- Warm-Up
- The $n = 3$ Case
- The $n \geq 4$ Case
- Conclusions

Graded Broadcast

Definition

Sender P_1 inputs v_1, every recipient P_i outputs (v_i, g_i) s.t.

- *Validity*: P_1 honest $\rightarrow \forall j : v_j = v_1 \ \wedge \ g_j = 1$
- *Consistency*: P_i honest, $g_i < n \rightarrow \forall j : v_j = v_i \ \wedge \ g_j \leq g_i + 1$

Intuition

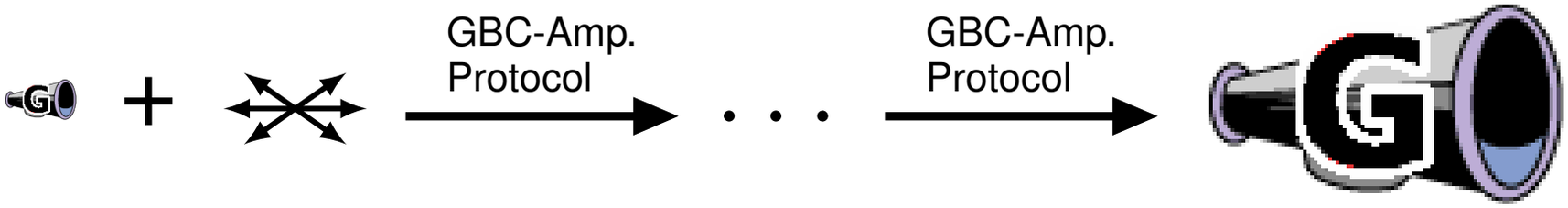
- Grade 1: Sender "looks" honest
- Grade 2: Sender is cheating, but other recipients might not know
- Grade 3: ... others know, but might not know that everybody knows
- ...

Roadmap for $n \geq 4$ Parties

1. Graded-Broadcast Amplification Protocol

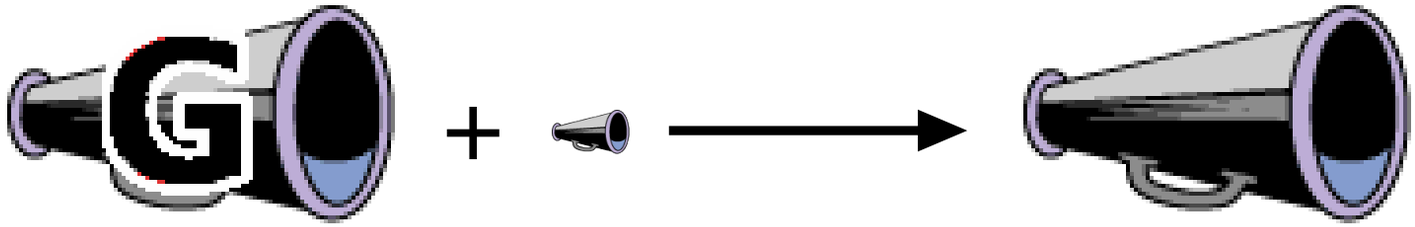
2

2. Recursion



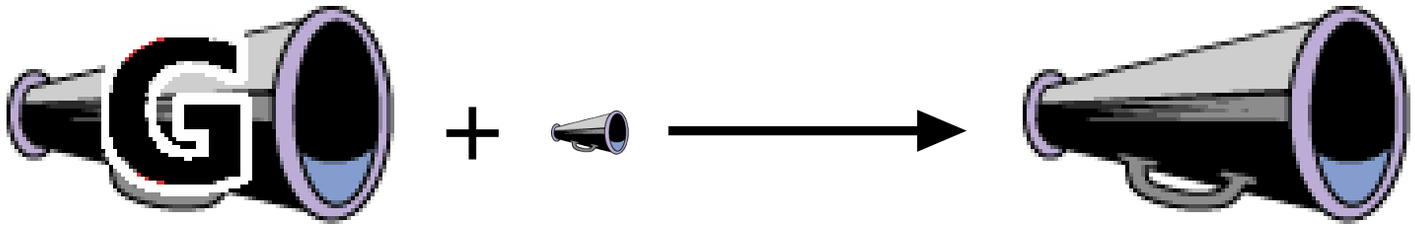
3

3. Graded Broadcast $\rightarrow$ Broadcast



1

Graded Broadcast $\rightarrow$ Broadcast



Protocol

0. P_i holds (v_i, g_i) (output from Graded Broadcast)
1. $\forall P_i$: g_i
2. $\forall Pi$: Accept $\begin{cases} v_i, & \text{if } \{1, \ldots, g_i\} \subseteq \{g_1, g_2, \ldots, g_n\} \\ \perp, & \text{otherwise} \end{cases}$

Analysis

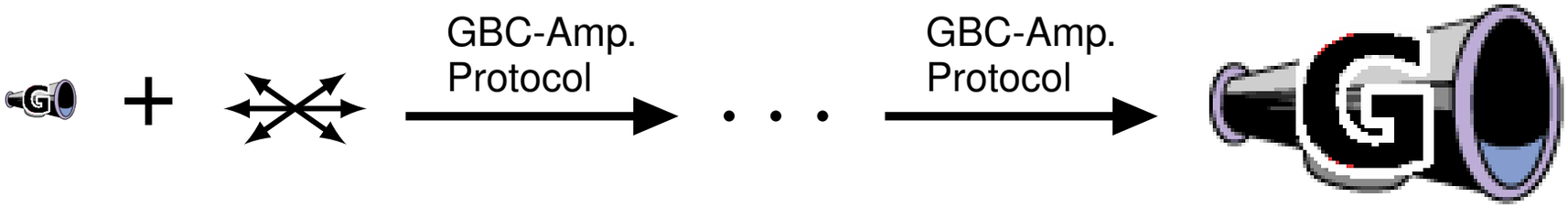
- *Validity:* Trivial because $\forall P_i : (v_i, g_i) = (v_1, 1)$
- *Consistency:*
  - Consider honest P_i accepting v_i with smallest g_i
  - Honest $P_j \rightarrow g_i < n \rightarrow v_j = v_i$ and $g_j \leq g_i + 1 \rightarrow$ accepts v_j

Roadmap for $n \geq 4$ Parties

1. Graded-Broadcast Amplification Protocol

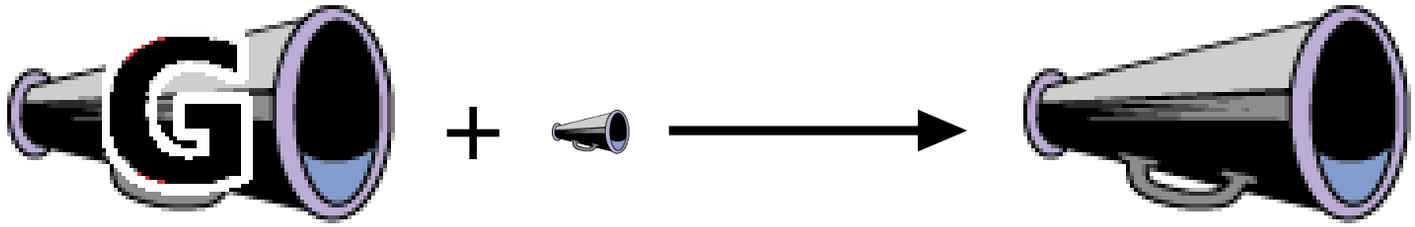
2

2. Recursion



3

3. Graded Broadcast $\rightarrow$ Broadcast



1 ✓

Hint Systems

Def: A *hint system* for domain D, set $S \subset D$, value $\widehat{v} \in S$:

$$G : (S, \widehat{v}) \to h \qquad V : (v, h) \to \{0, 1\}$$

such that for $h \leftarrow G(S, \widehat{v})$, $\forall v \in S : V(h, v) \Leftrightarrow (v = \widehat{v})$

Intuition

- For each S, $\widehat{v}$, there *exists* a hint h s.t.
  - $\widehat{v}$ is accepted by h, and
  - Every $v \in S \setminus \{\widehat{v}\}$ is rejected by h

Properties (totally trivial)

- For any set S and a hint h, either
  - h supports no value in S,
  - h supports one value in S, or
  - h supports multiple values in S

Hints from Universal Hashing

Def: A *hint system* for domain D, set $S \subset D$, value $\widehat{v} \in S$:

$$G : (S, \widehat{v}) \to h \qquad V : (v, h) \to \{0, 1\}$$

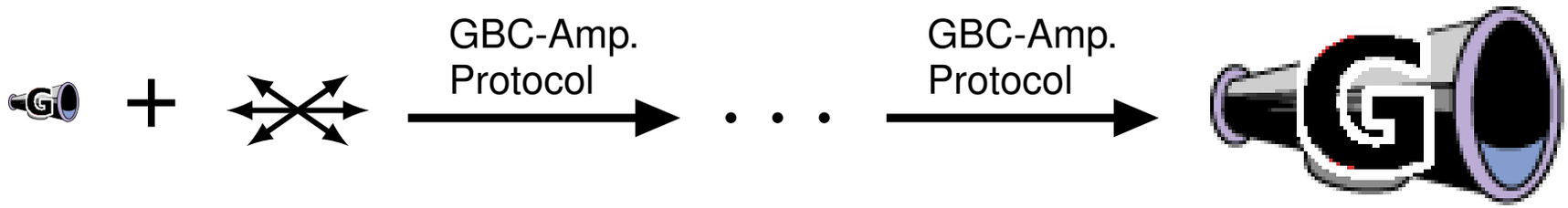
such that for $h \leftarrow G(S, \widehat{v})$, $\forall v \in S : V(h, v) \Leftrightarrow (v = \widehat{v})$

Construction (for $D = \{0, 1\}^\ell$)

- For fixed k, interpret $v \in D$ as polynomial over $\mathsf{GF}(2^k)$ (degree ℓ/k)
- **Idea:** Hint $h = (x, y)$ s.t. $\forall v \in S : f_v(x) = y \Leftrightarrow (v = \widehat{v})$
- For $v \neq \widehat{v}$, $f_{\widehat{v}}$ and f_v coincide in at most ℓ/k positions
- For set S, $f_{\widehat{v}}$ and f_v for any $v \in S$ coincide in at most $|S|\ell/k$ positions
- Choose k such that $2^k > |S|\ell/k$, e.g. $k = \log(|S|\ell)$
- Hint $h = (x, f_{\widehat{v}}(x))$ for x which does not coincide within S

Analysis: Hint size: $2\log(|S|\ell)$ bits.

Graded-Broadcast Amplification



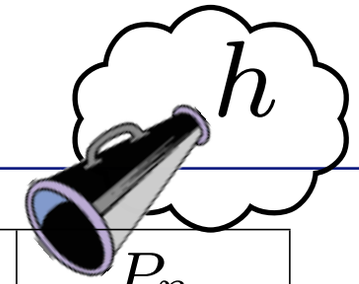
The Protocol (Sketch)

0. Sender P_1 holds v_1, recipients P_i hold nothing

1. – $2n$. Every P_i sends to every P_j all values he has seen so far

$2n$+1. Sender P_1 hint h, recipients P_i decide on (v_i, g_i)

Graded Broadcast – A Protocol Execution



Rd	P_1	P_2	$\cdots$	P_i	$\cdots$	P_n
0	$\{v_1\}$					
1		$S_{2,1}$		$S_{i,1}$		$S_{n,1}$
2		$S_{2,2}$		$S_{i,2}$		$S_{n,2}$
3		$S_{2,3}$		$S_{i,3}$		$S_{n,3}$
4		$S_{2,4}$		$S_{i,4}$		$S_{n,4}$
$\vdots$		$\vdots$		$\vdots$		$\vdots$
$2n-2$		$S_{2,2n-2}$		$S_{i,2n-2}$		$S_{n,2n-2}$
$2n-1$		$S_{2,2n-1}$		$S_{i,2n-1}$		$S_{n,2n-1}$
$2n$	$S_{1,2n}$					

Grade: $g_i = \min g$ s.t. $S_{i,g} \ldots S_{i,2n-g}$ are green

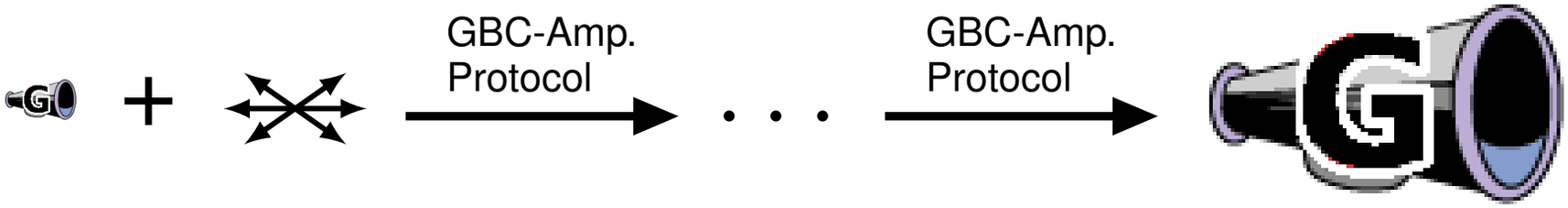
Analysis:
- Validity: trivial
- Consistency: think :-)

Roadmap for $n \geq 4$ Parties

1. Graded-Broadcast Amplification Protocol

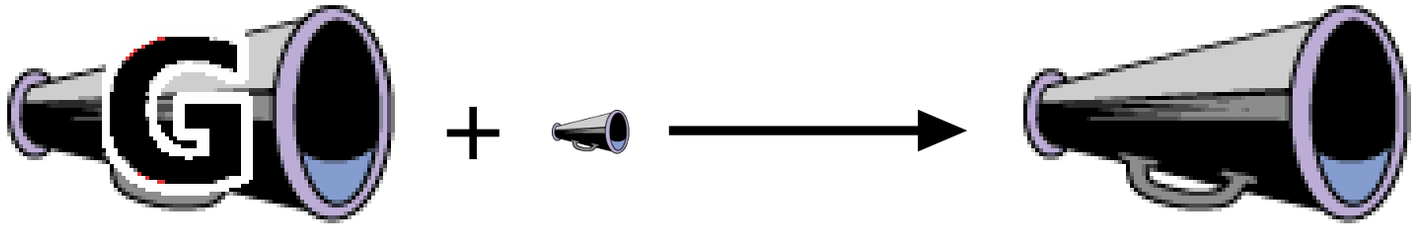
2 ✓

2. Recursion



3 ✓

3. Graded Broadcast $\rightarrow$ Broadcast



1 ✓

The $n \geq 4$ Case

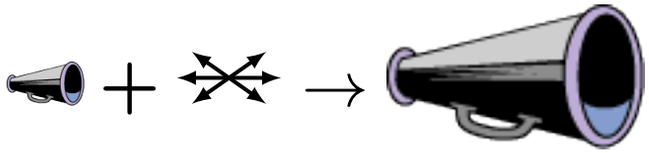
Putting things together

- Observe: $|S_{1,2n}| \leq n^{2n}$
- Hint size for S: $2\log(|S|\ell)$ bits
- Needed hint size: $2\log(n^{2n}\ell) = 4n\log n + 2\log \ell$ bits
- Recursion: Hint size $7n\log n$ bits
- Graded Broadcast $\rightarrow$ Broadcast: another $n\log n$ bits
- Grand total: $\boldsymbol{8n\log n}$ bits

Conclusions

$n = 3$

- Domain size 3 (1.6 bits) is sufficient for arbitrary broadcasts
- Domain size 2 (1 bit) is not sufficient
- $\phi_3(\cdot) = 3$



$n \geq 4$

- $8n \log n$ bits is sufficient for arbitrary broadcasts
- $n - 3$ bits is not sufficient
- $n - 3 \;\leq\; \log \phi_n(\cdot) \;\leq\; 8n \log n$

Remarks

- Communication through  is independent of ℓ
- Perfect security