Empirical DNS Padding Policy

Daniel Kahn Gillmor <dkg@aclu.org>

NDSS DPRIVE workshop 2017
San Diego, CA

Cleartext DNS Traffic

Queries	Responses
alice?	alice:17
bob?	bob:25,96
charlie?	charlie:21
david?	david:14,22
charlie?	charlie:21
edward?	edward:58
frances?	frances:13

Confidential DNS Traffic

Queries	Responses
******	********
****	*********
********	**********
******	***********
********	**********
*******	*********
********	**********

Note: independent of encryption mechanism…

Padding Mechanism

- RFC 7830: EDNS(0) Padding Option
  - Alexander Mayrhofer, http://edns0-padding.org/

```
0                       8                      16
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                  OPTION-CODE                  |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|                 OPTION-LENGTH                 |
+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+--+
|        (PADDING) ...        (PADDING) ...     /
+-  -  -  -  -  -  -  -  -  -  -  -  -  -  -  -
```

Possible Padding Policies

- No padding
- Random padding
- Pad to next closest multiple of some blocksize
- Pad to next closest power of some base
- Max out the MTU
- Pad to blocksize plus some random number of extra blocks
- …

Bad or Impossible Padding Policies

- Pad a fixed (non-zero) amount
- Negative padding
- Pseudo-random padding
- Max out the DNS TCP message size
- …

Padding Variations

- Should response padding take into account query padding?
- Minimum size to sweep up all small messages
- …

Measurements

- Bandwidth cost
  - Cost to defenders
  - Rough proxy for latency, delivery failure
- Followup cost
  - Cost to attacker
  - How many other Q/R pairs could be mixed in with a targeted Q/R pair?

β – Bandwidth cost

- Bandwidth cost
  - Cost to defenders
  - Rough proxy for latency, delivery failure
  - Add up padded sizes, normalize by unpadded cost

$$\beta = \frac{\sum_{x,y} (x+y) P_{x,y}}{\sum_{x,y} (x+y) U_{x,y}}$$

Φ – Followup cost

- Followup cost
  - Cost to attacker (passive monitor) interested in one particular Q/R pair.
  - Attacker sees only padded sizes.
  - How many other Q/R pairs could be mixed in with the target?

$$\phi = \frac{\sum_{i,j,x,y \mid T_{i,j\rightarrow x,y} > 0} \left(U_{i,j} P_{x,y} \right)}{N^2}$$

Confidential DNS Traffic

Queries	Responses
******	********
****	*********
********	**********
******	***********
********	**********
*******	*********
********	**********

DNS Traffic Sizes

Queries	Responses
6	8
4	9
8	10
6	11
8	10
7	9
8	10

DNS Q/R size counts
unpadded

Response Size						
12						
11			1			
10					3	
9	1			1		
8			1			
	4	5	6	7	8	9

Query Size

β: 1.0

Φ: 0.26

DNS Q/R size counts
`blk(2)`

Response Size

12			1			
11						
10			1		4	
9						
8			1			
	4	5	6	7	8	9

Query Size

β: 1.05

Φ: 0.39

DNS Q/R size counts

`blk(3)`

Response Size

12			1			3
11						
10						
9			2			1
8						
	4	5	6	7	8	9

Query Size

β: 1.13

Φ: 0.31

DNS Q/R size counts

`q:blk(3),r:blk(2)`

Response Size	4	5	6	7	8	9
12			1			
11						
10			1			4
9						
8			1			

Query Size

β: 1.09

Φ: 0.39

DNS Q/R size counts
`q:blk(8),r:blk(12)`

Response Size

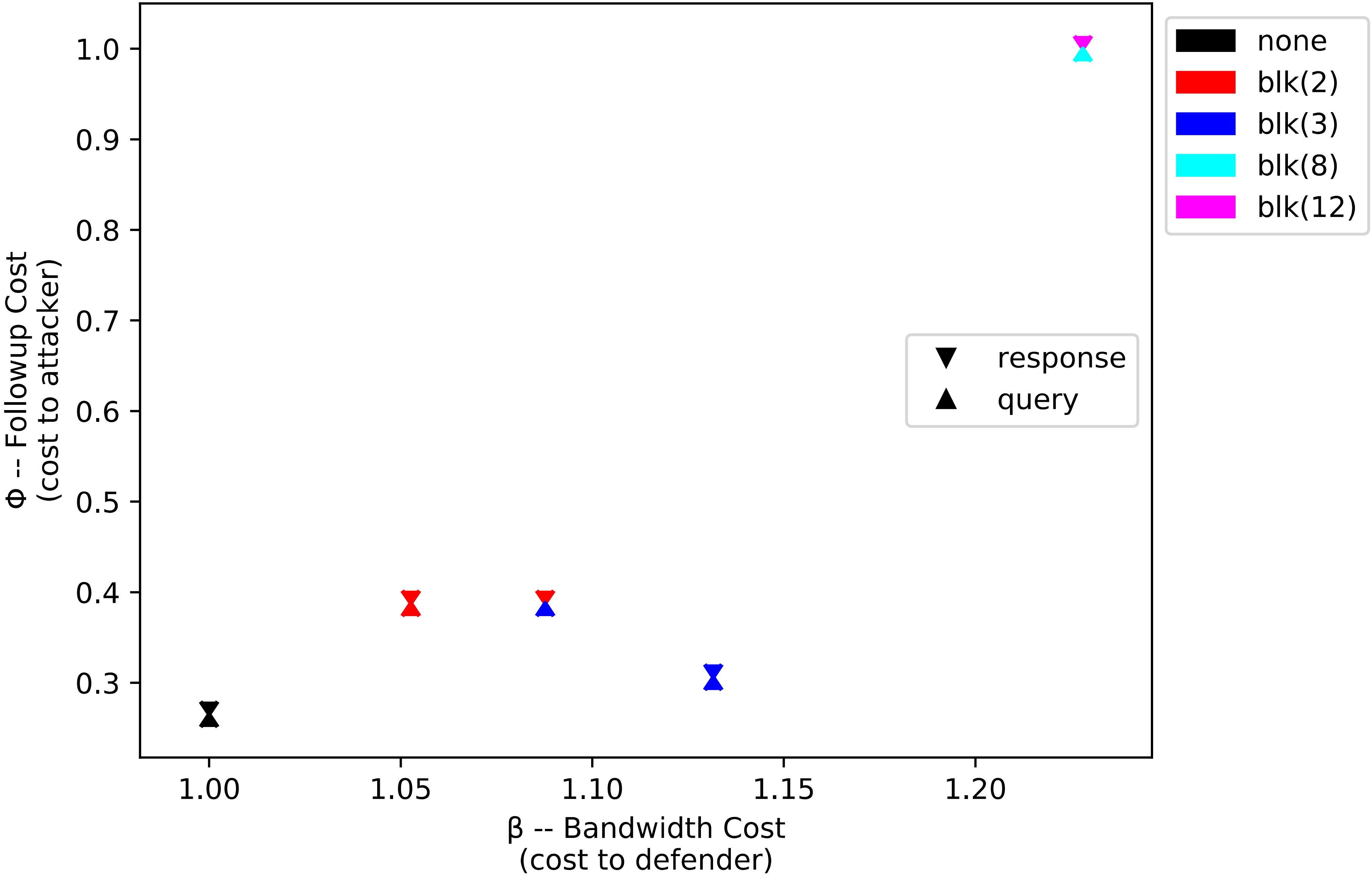
12					7	
11						
10						
9						
8						
	4	5	6	7	8	9

Query Size

β: 1.23

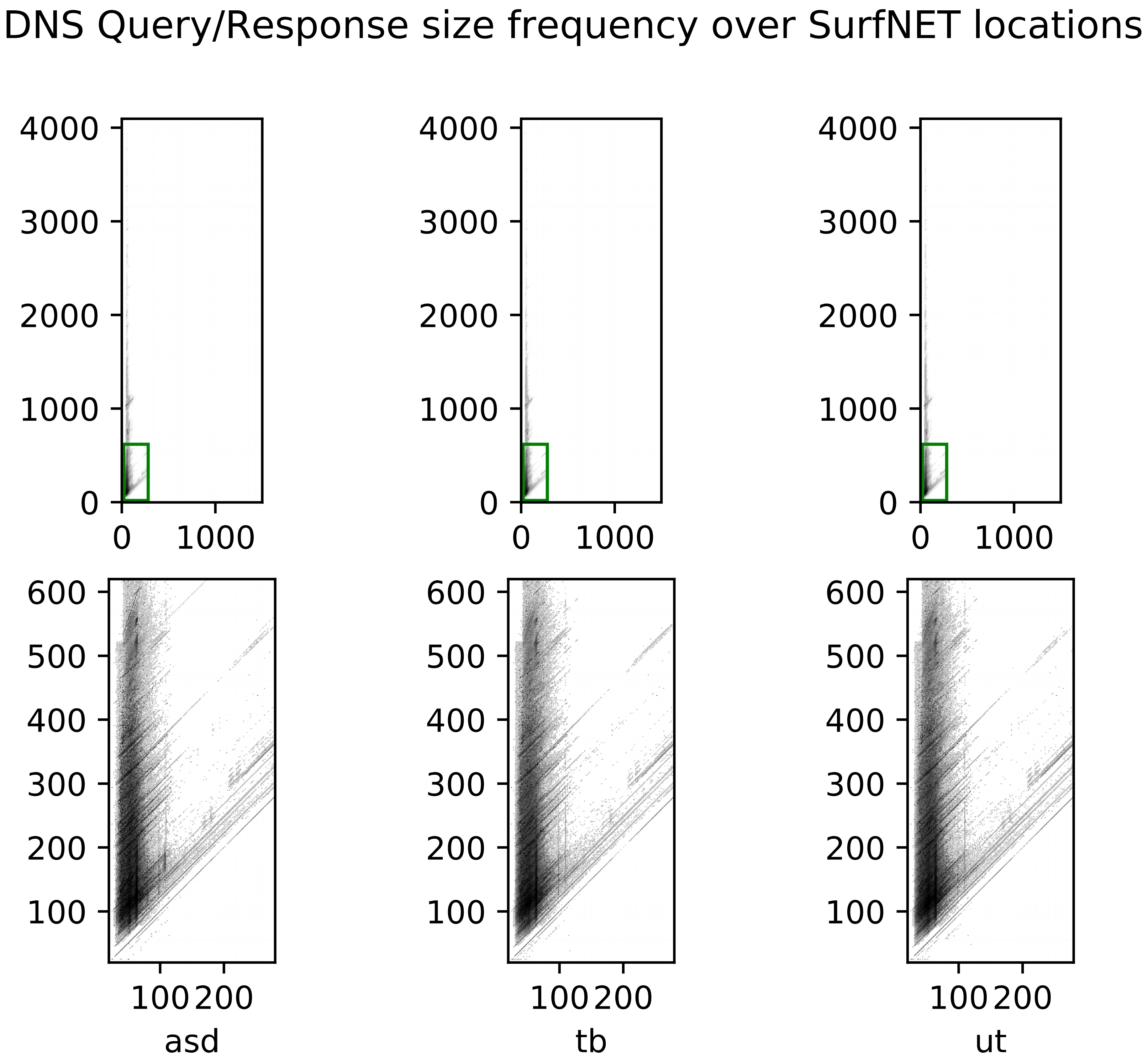
Φ: 1.0

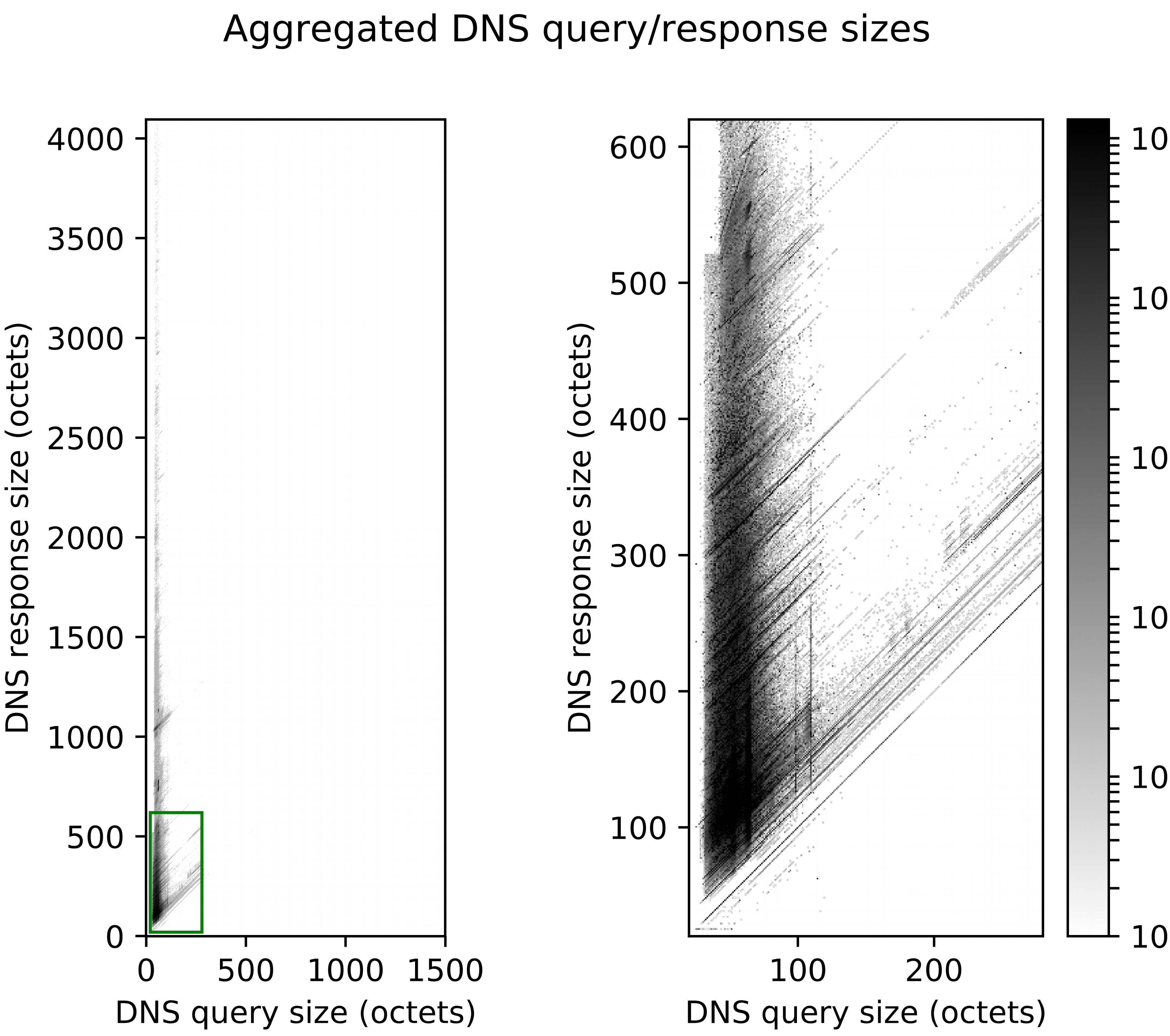
Padding Policy Evaluation (example)



Data from the wild

- Cleartext DNS Query/Response pair counts by size
- Gathered from 3 different SurfNET recursive resolvers over the course of a week
  - https://github.com/SURFnet/eemo
- Thanks to Roland van Rijswijk-Deij!


DNS Query/Response size frequency over SurfNET locations
4000
3000
2000
1000
0
0
1000
600
500
400
300
200
100
100
200
asd
tb
ut

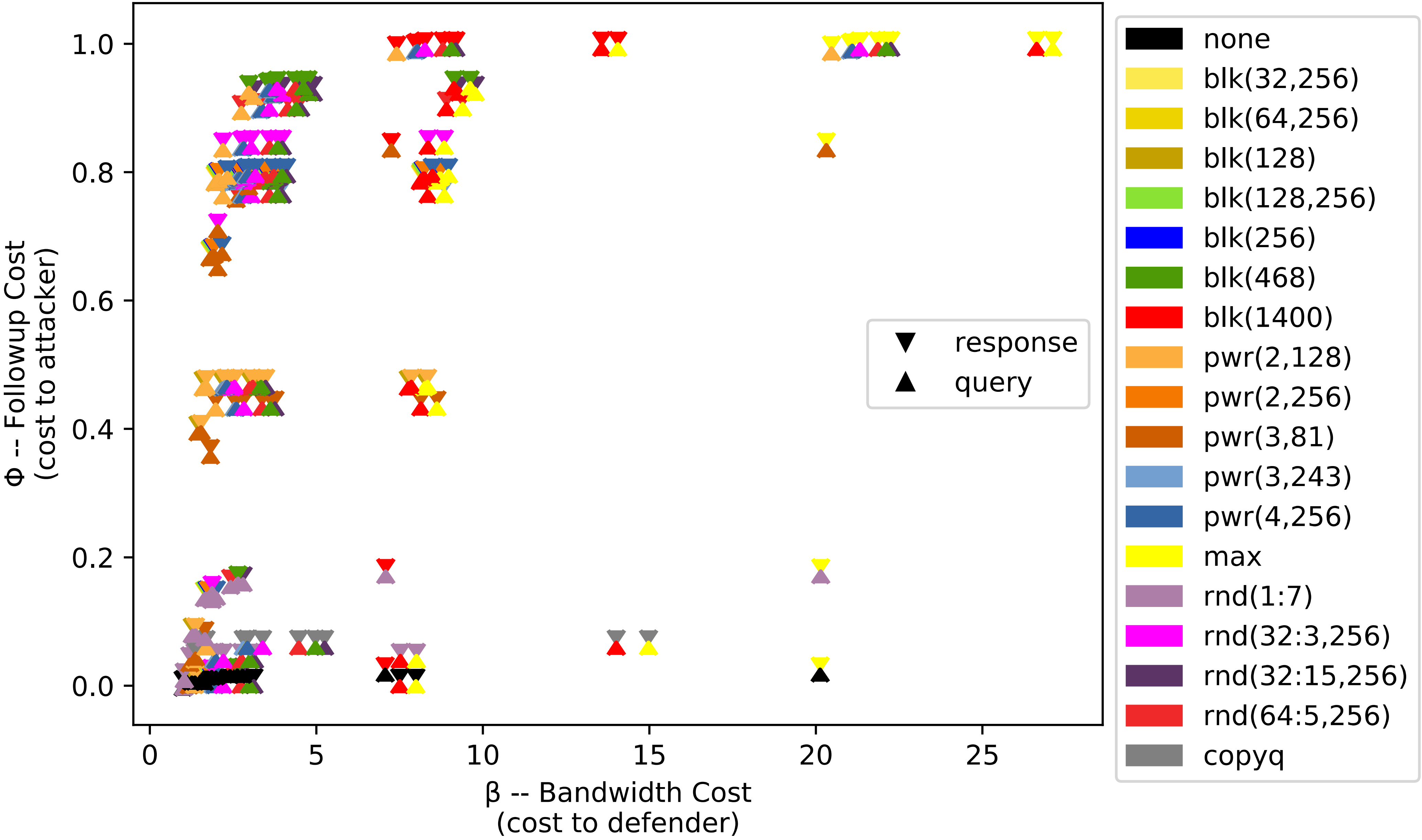


Aggregated DNS query/response sizes
DNS response size (octets)
0
500
1000
1500
2000
2500
3000
3500
4000
DNS query size (octets)
0
500
1000
1500
DNS response size (octets)
100
200
300
400
500
600
DNS query size (octets)
100
200
10^0
10^1
10^2
10^3
10^4
10^5

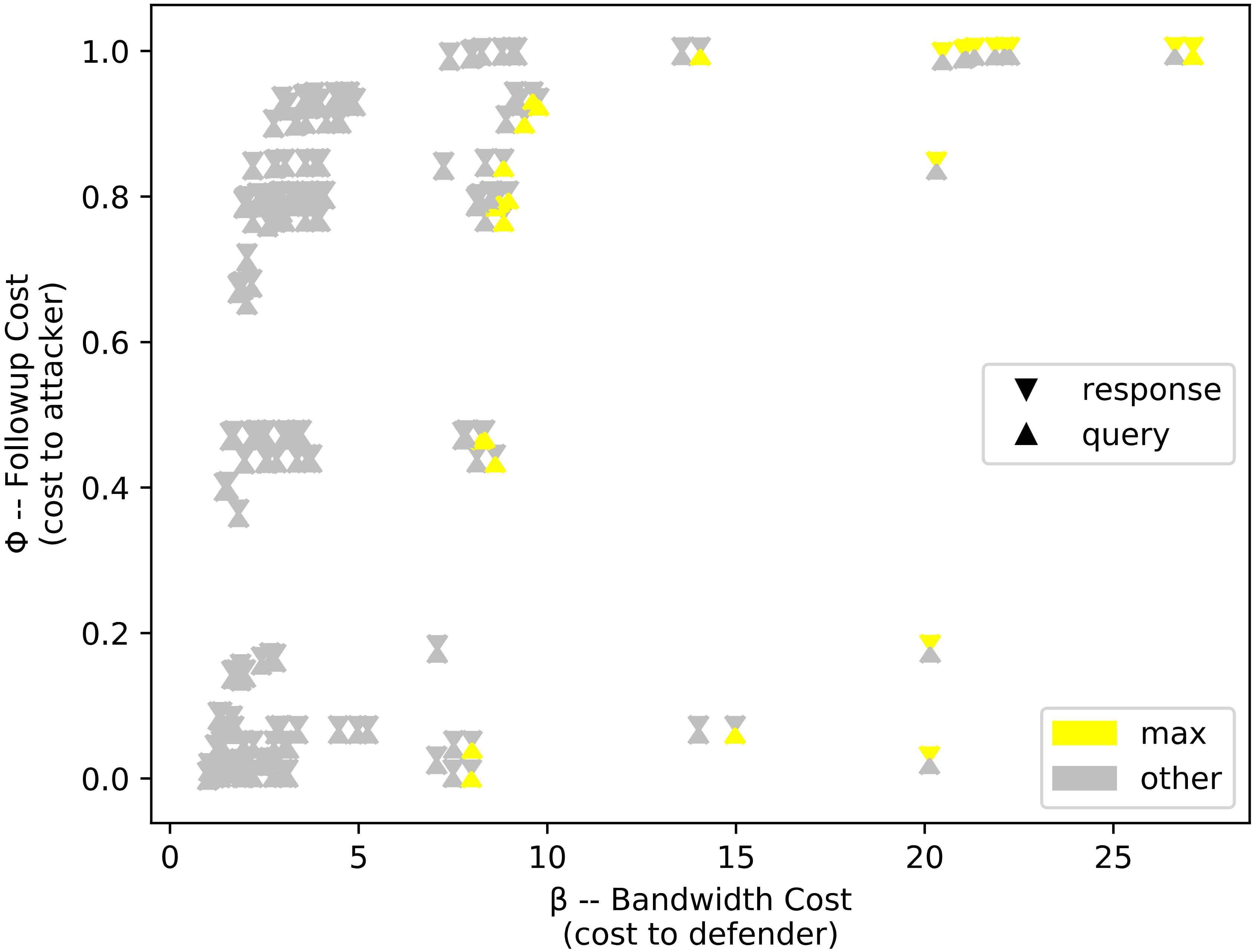
Padding Schemes

- **`blk(sz[,min])`** – pad to blocks of size **`sz`**, starting at **`min`**.
- **`pwr(b[,min])`** – pad to powers of base **`b`**, starting at **`min`**.
- **`max`** – pad queries to 1500, responses to 4096
- **`rnd(sz:blks[,min])`** – pad to blocks of size **`sz`**, starting at **`min`**, plus up to **`blks`** extra blocks (uniformly at random)
- **`copyq`** – pad responses by amount of query padding

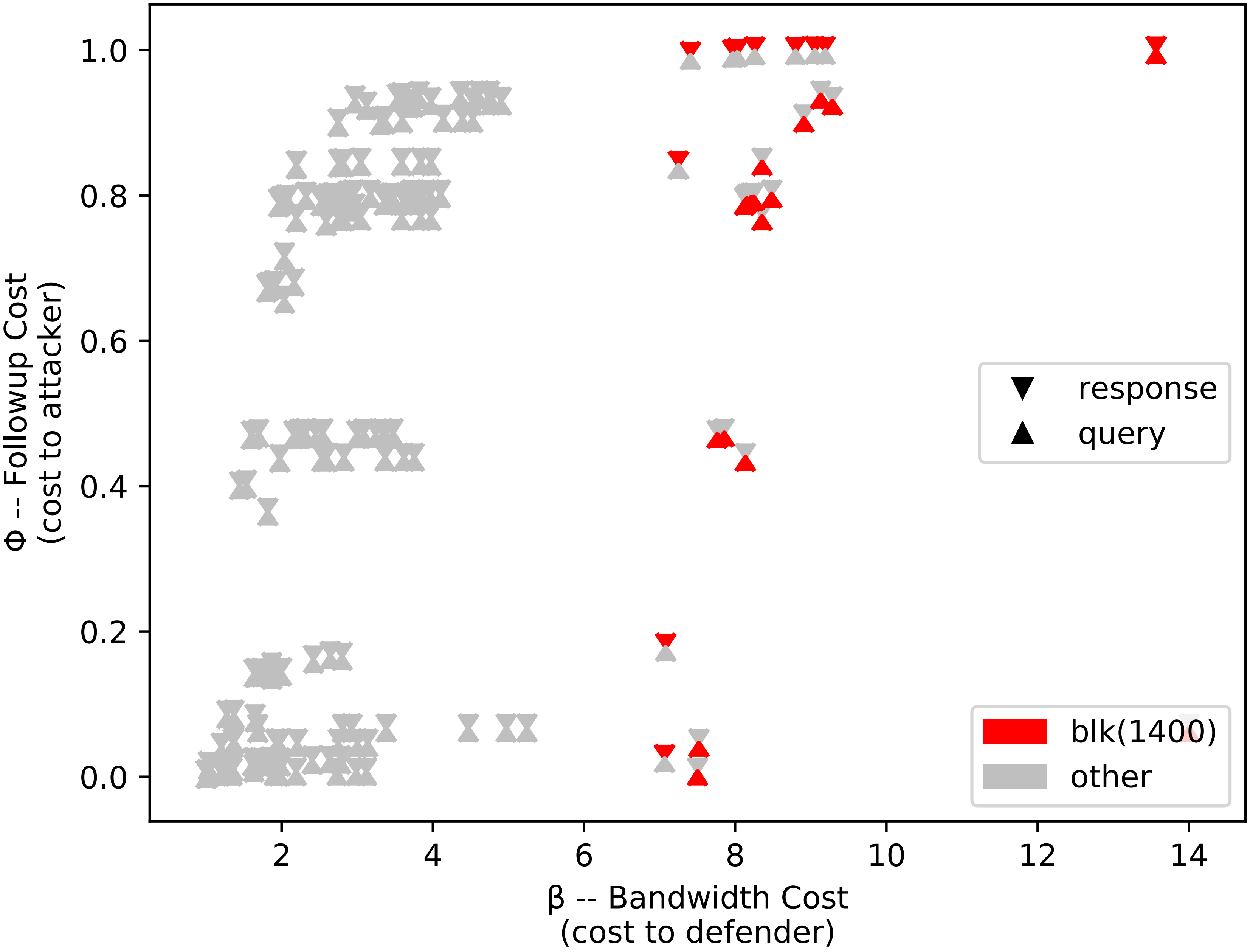
Combinations of all schemes



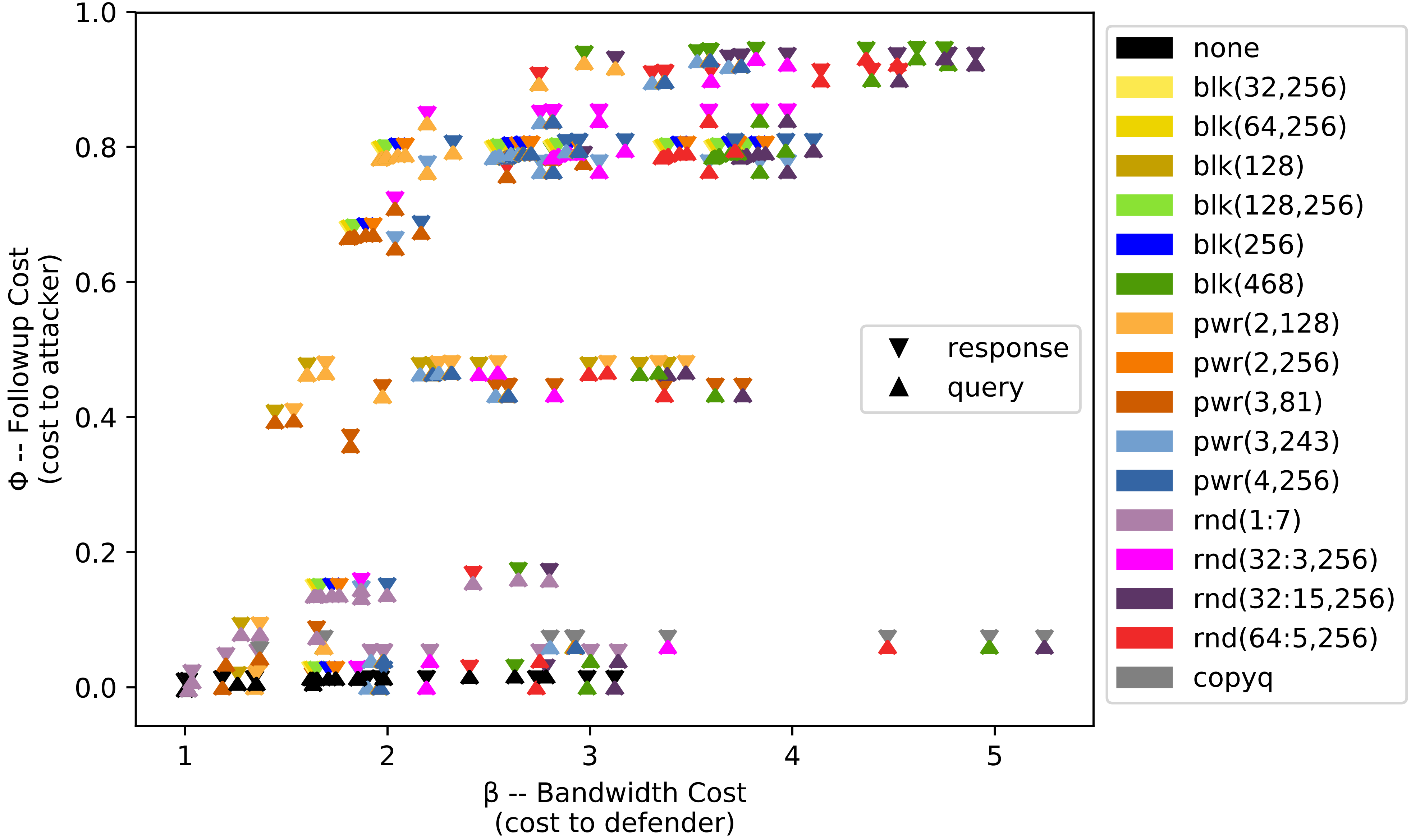
max is Wasteful



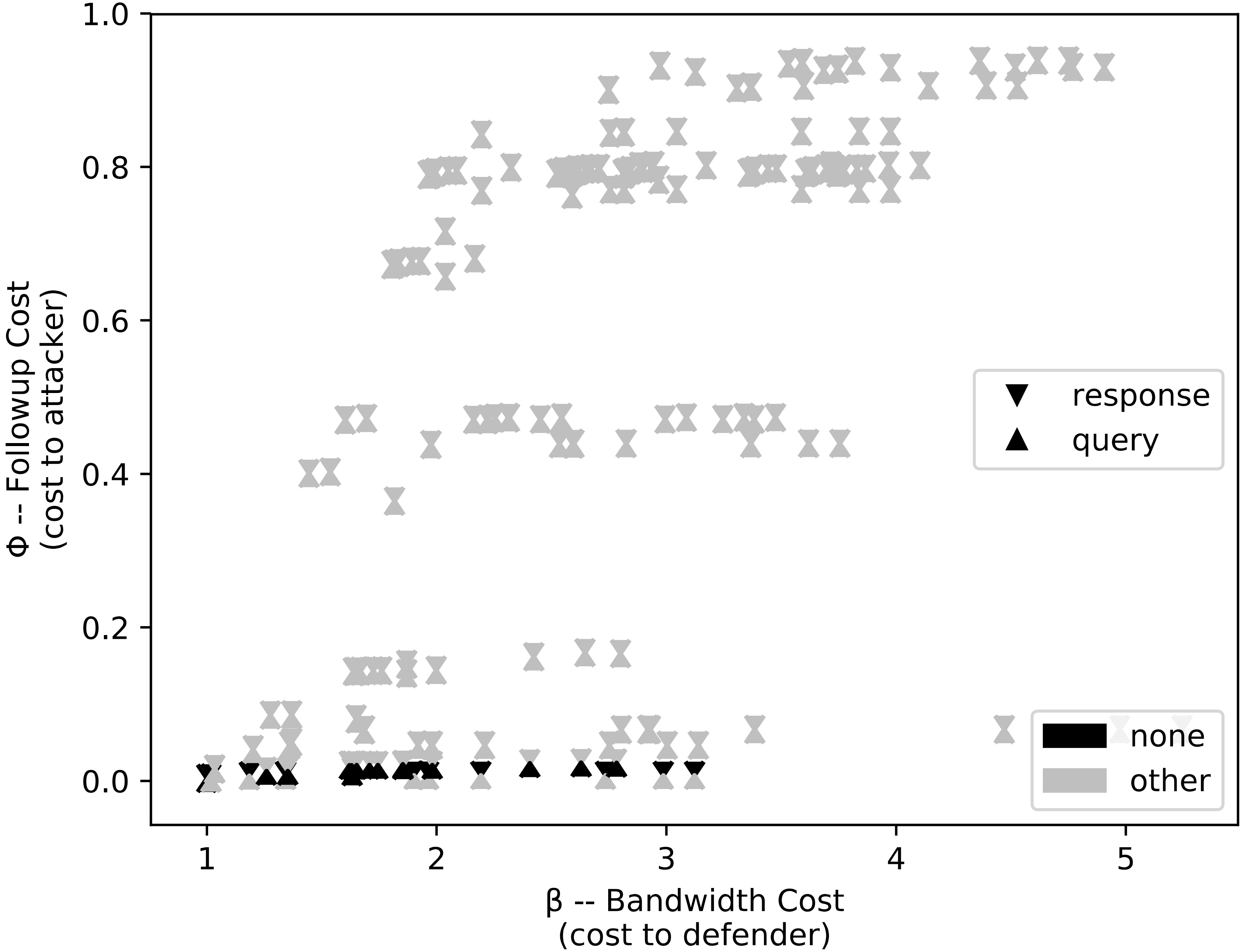
`blk(1400)` is Expensive



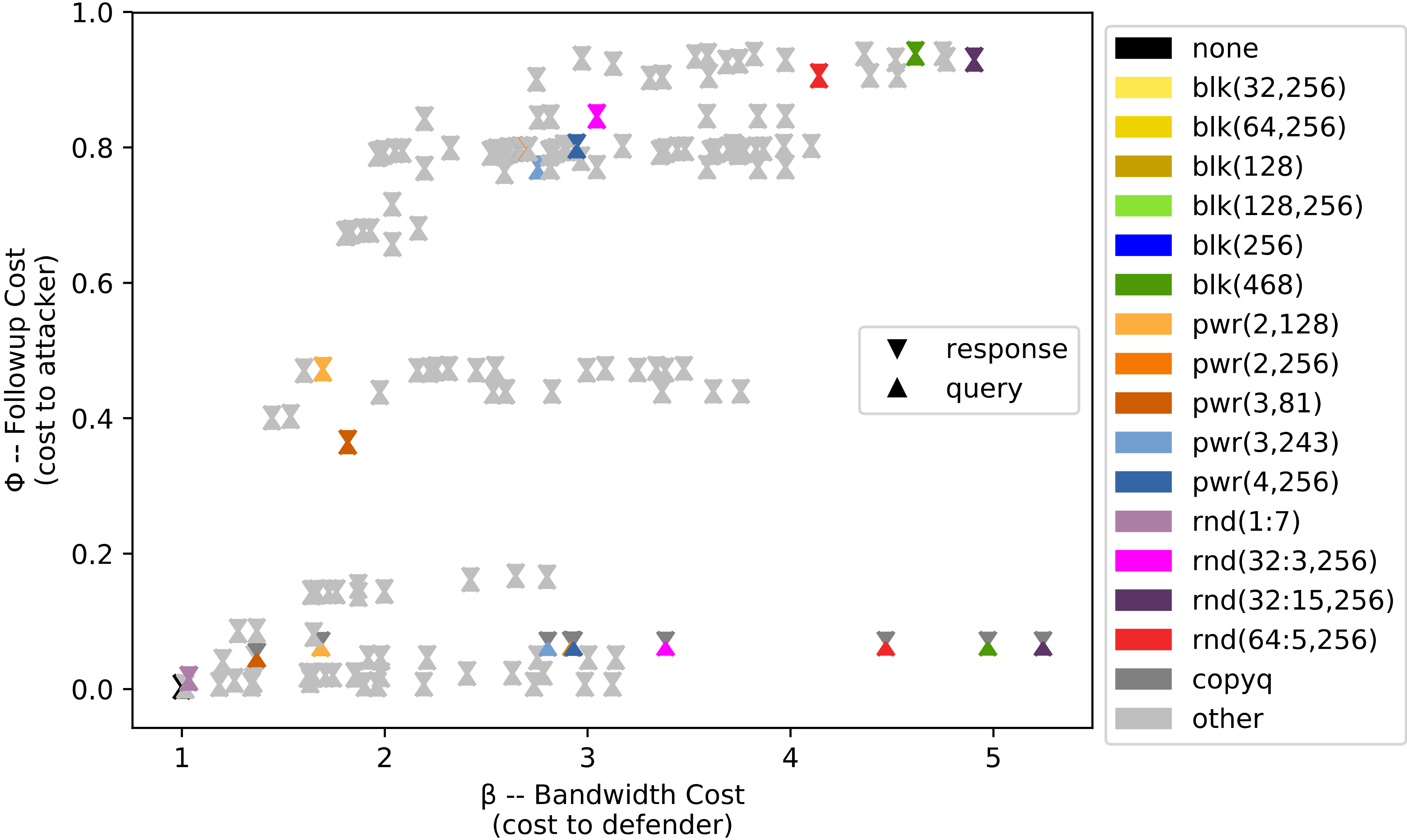
Into the Details



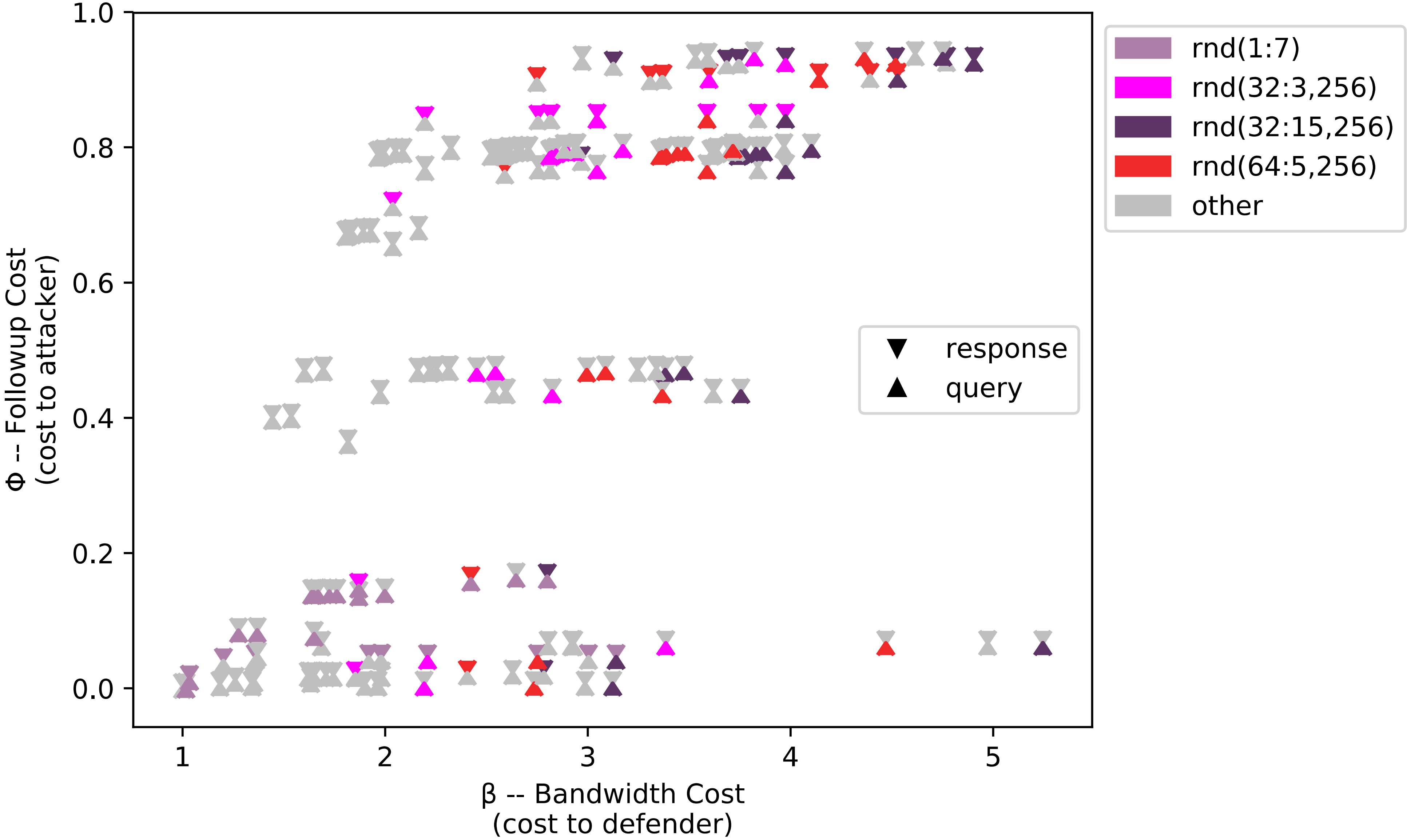
Both Sides Need To Pad



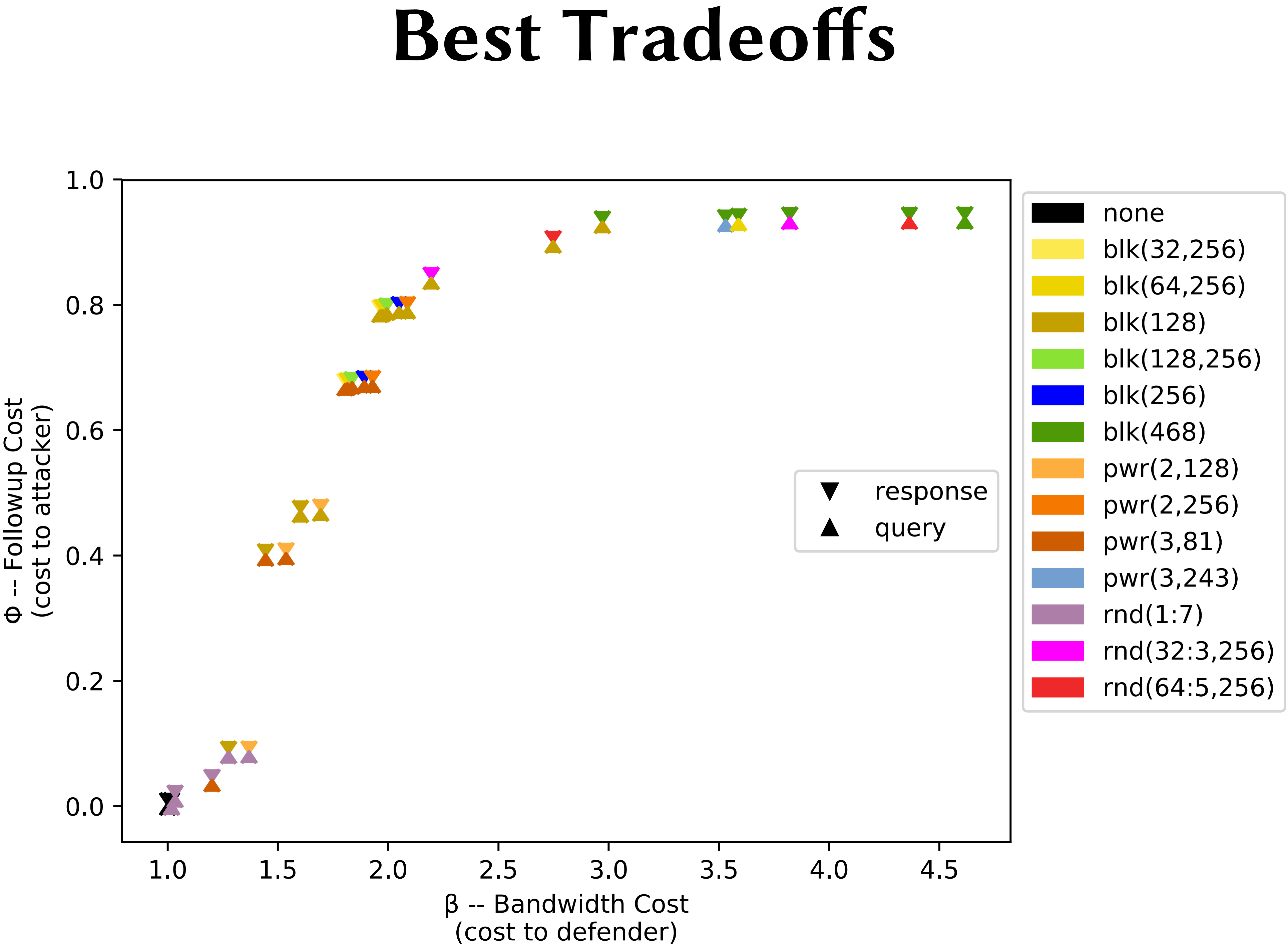
When the Same...



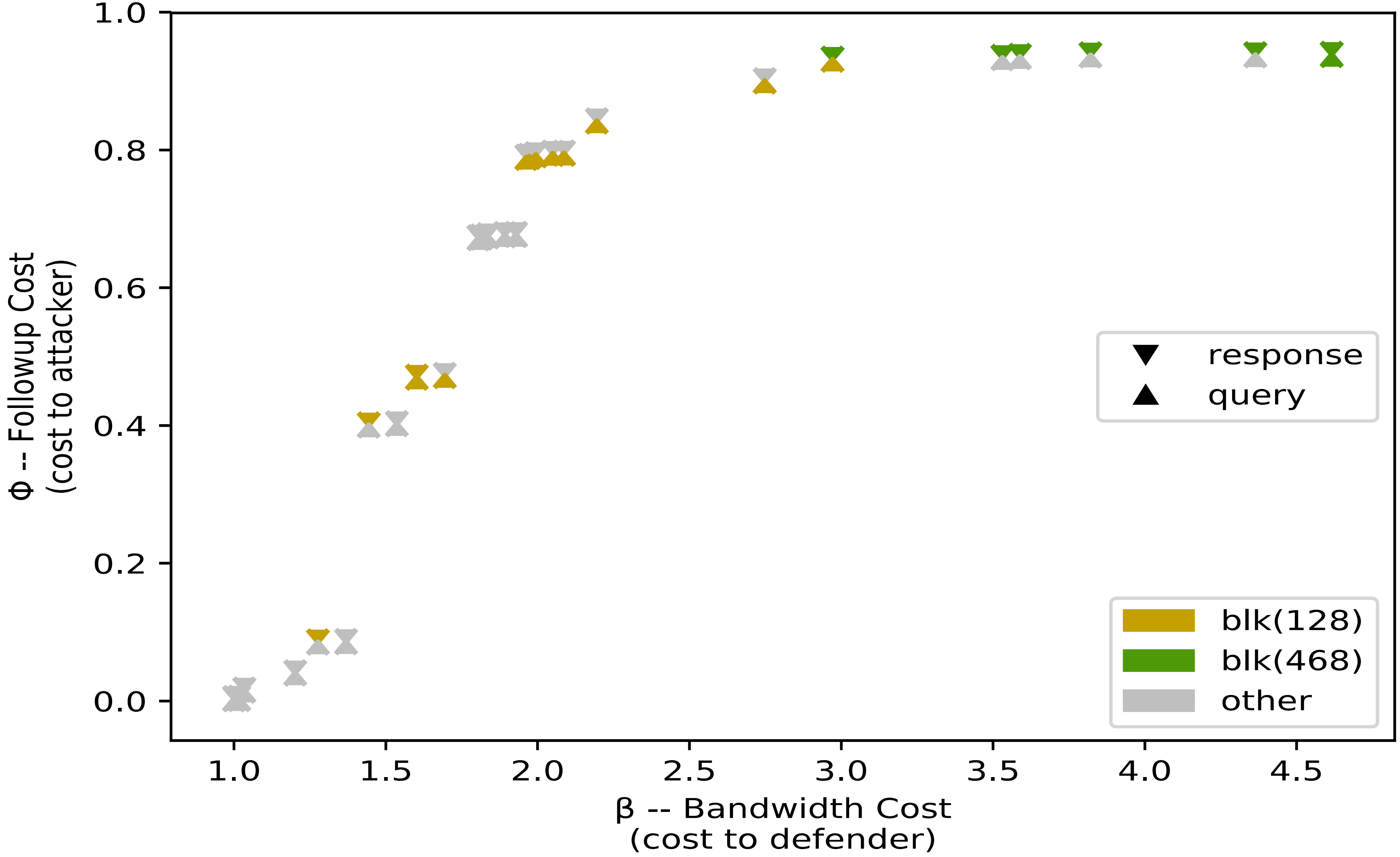
Randomness



1.0
0.8
0.6
0.4
0.2
0.0
Φ -- Followup Cost
(cost to attacker)
1
2
3
4
5
β -- Bandwidth Cost
(cost to defender)
rnd(1:7)
rnd(32:3,256)
rnd(32:15,256)
rnd(64:5,256)
other
▼ response
▲ query


Best Tradeoffs
Φ -- Followup Cost
(cost to attacker)
1.0
0.8
0.6
0.4
0.2
0.0
1.0
1.5
2.0
2.5
3.0
3.5
4.0
4.5
β -- Bandwidth Cost
(cost to defender)
▼ response
▲ query
none
blk(32,256)
blk(64,256)
blk(128)
blk(128,256)
blk(256)
blk(468)
pwr(2,128)
pwr(2,256)
pwr(3,81)
pwr(3,243)
rnd(1:7)
rnd(32:3,256)
rnd(64:5,256)

Recommendations



Observations

- Padding is only useful when both sides pad.
- Responses include queries, but response padding doesn’t need to consider query padding.

Recommendations

- Clients should pad queries to the closest multiple of 128 octets.
- If a recursive resolver sees padding in a query, it should pad its response to a multiple of 468 octets.
- There is little gain from padding responses to unpadded queries.

Devilish Details

- Encryption layer will have some overhead, which puts additional pressure on the MTU.
- Empirical evidence is contingent on the dataset.
- Changes to common DNS practice (e.g. wider deployment of DNSSEC) will affect these conclusions.
- The padding imbalance between client and server might imply an amplification attack useful in a DDoS; these recommendations are for established sessions only.

Further Research

- Defense against active attackers
- Q/R data, not just sizes
- Alternate evaluation functions
  - Penalize exceeding MTU
  - Mutual entropy of cleartext and sizes
- Correlations between successive Q/R pairs
- Time-series data
- …

Thanks!

- Alexander Mayrhofer
- Roland van Rijswijk-Deij
- Sara Dickinson
- Shane Kerr