Visualizing size-security tradeoffs for lattice-based encryption

Daniel J. Bernstein

Horizontal axis: ciphertext size

Why focus on size instead of CPU time?

— Fitting into existing frameworks and protocols. Data from Google. Long term: Hardware trends.

Horizontal axis: ciphertext size

Why focus on size instead of CPU time?

— Fitting into existing frameworks and protocols.
Data from Google. Long term: Hardware trends.

Which size metric to use?
e.g. `ntrulpr` beats `sntrup` in key size,
but `sntrup` beats `ntrulpr` in ciphertext size.

Horizontal axis: ciphertext size

Why focus on size instead of CPU time?

— Fitting into existing frameworks and protocols.
Data from Google. Long term: Hardware trends.

Which size metric to use?
e.g. `ntrulpr` beats `sntrup` in key size,
but `sntrup` beats `ntrulpr` in ciphertext size.

— Google's 2016 experiment used key+ciphertext.

Horizontal axis: ciphertext size

Why focus on size instead of CPU time?

— Fitting into existing frameworks and protocols. Data from Google. Long term: Hardware trends.

Which size metric to use?
e.g. `ntrulpr` beats `sntrup` in key size,
but `sntrup` beats `ntrulpr` in ciphertext size.

— Google's 2016 experiment used key+ciphertext. But long term: Use IND-CCA2 to multicast+cache public keys (2015 McGrew). Lattice traffic is then much closer to ciphertext than to key+ciphertext.

Vertical axis: Core-SVP security estimate

Beware (potential/actual) oversimplifications inside lattice security estimates. Can lead to:

- Overstating security.
- Understating security—damaging deployment.
- Damaging comparisons: e.g. omitting "hybrid attacks"; e.g. overstating `sntrup` "rotations".

Vertical axis: Core-SVP security estimate

Beware (potential/actual) oversimplifications inside lattice security estimates. Can lead to:

- Overstating security.
- Understating security—damaging deployment.
- Damaging comparisons: e.g. omitting "hybrid attacks"; e.g. overstating `sntrup` "rotations".

Security estimate where (claimed) data points are easiest to find: "Core-SVP" pre-quantum estimate.

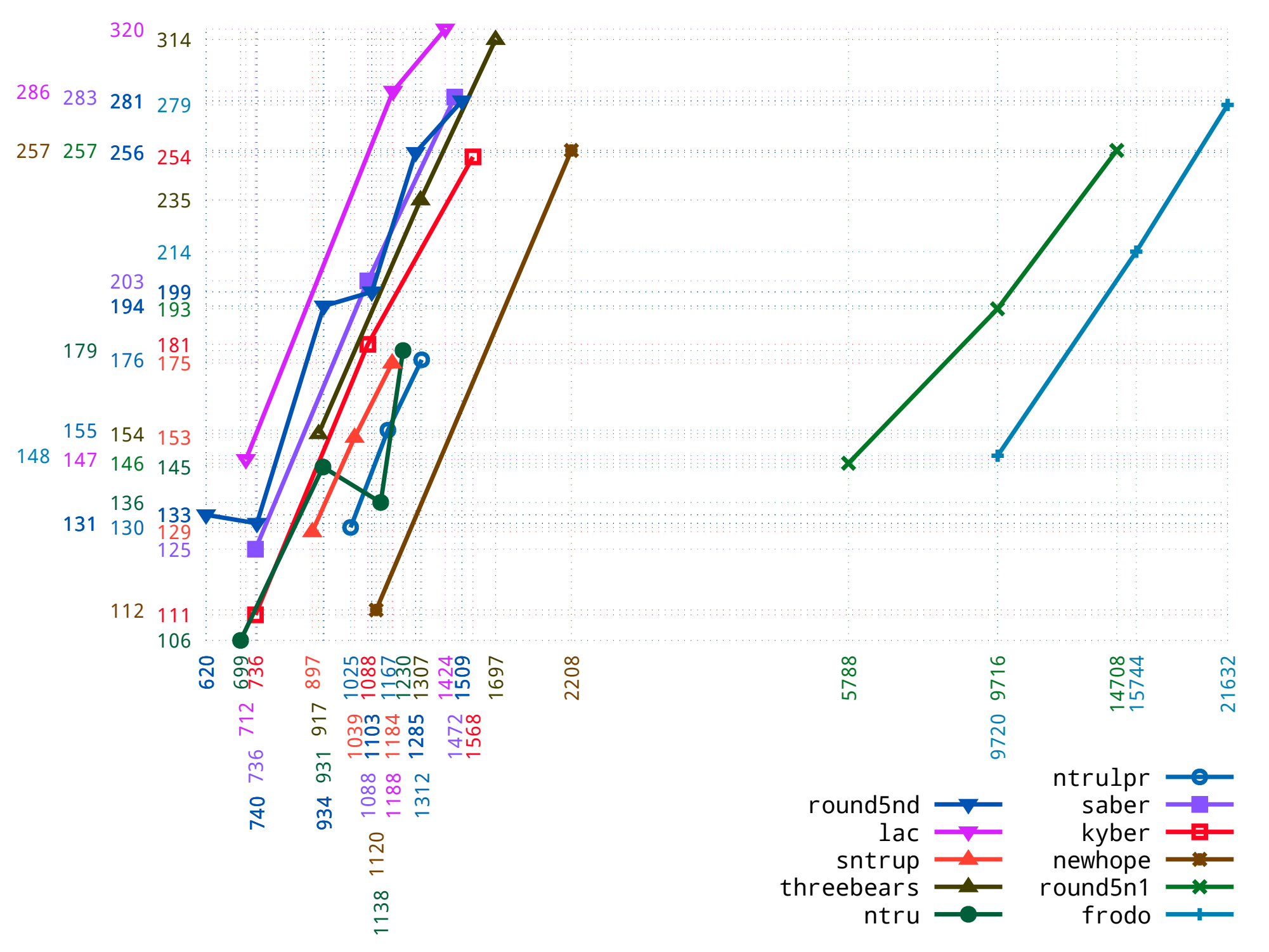
Vertical axis: Core-SVP security estimate

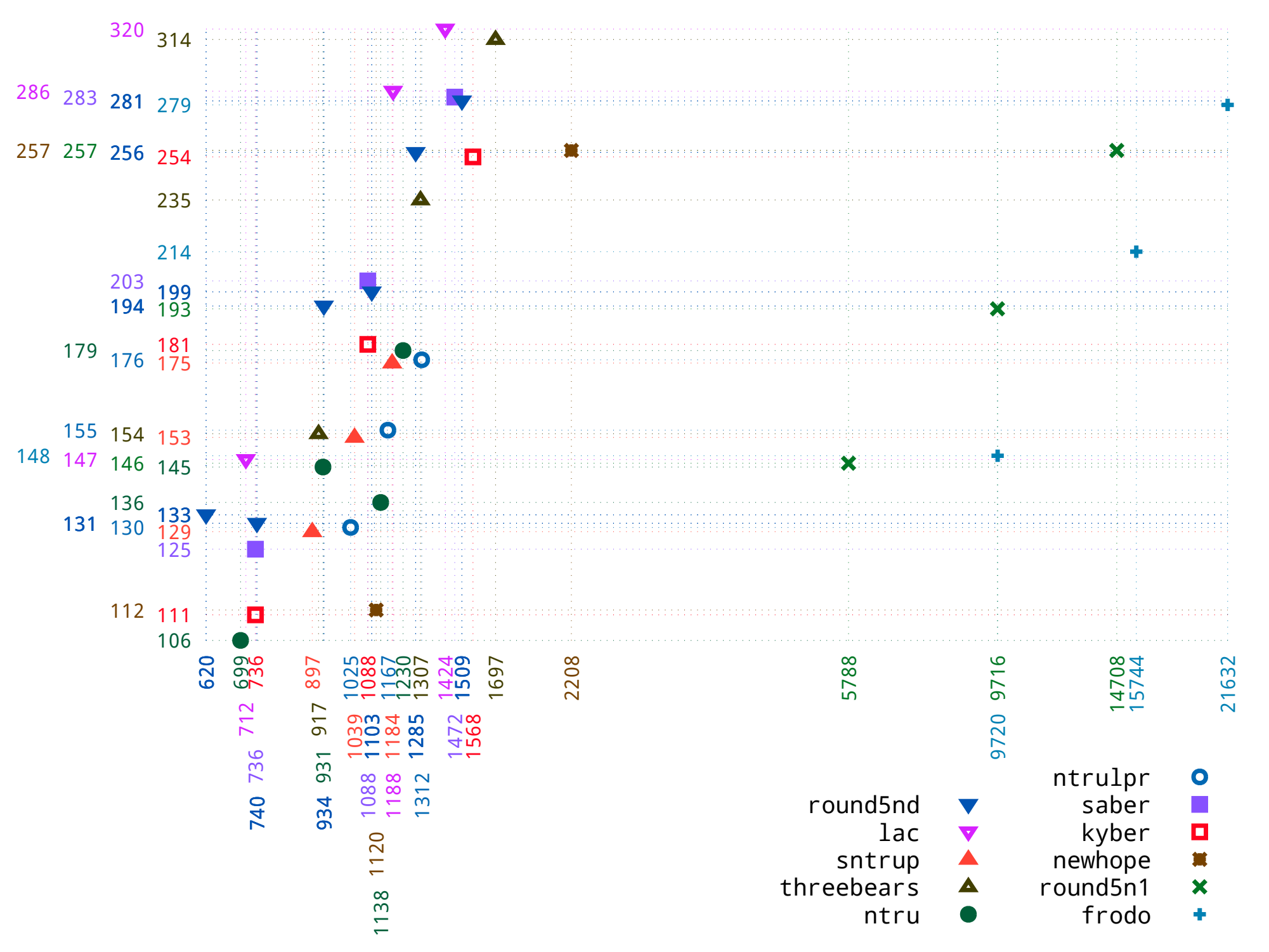
Beware (potential/actual) oversimplifications inside lattice security estimates. Can lead to:

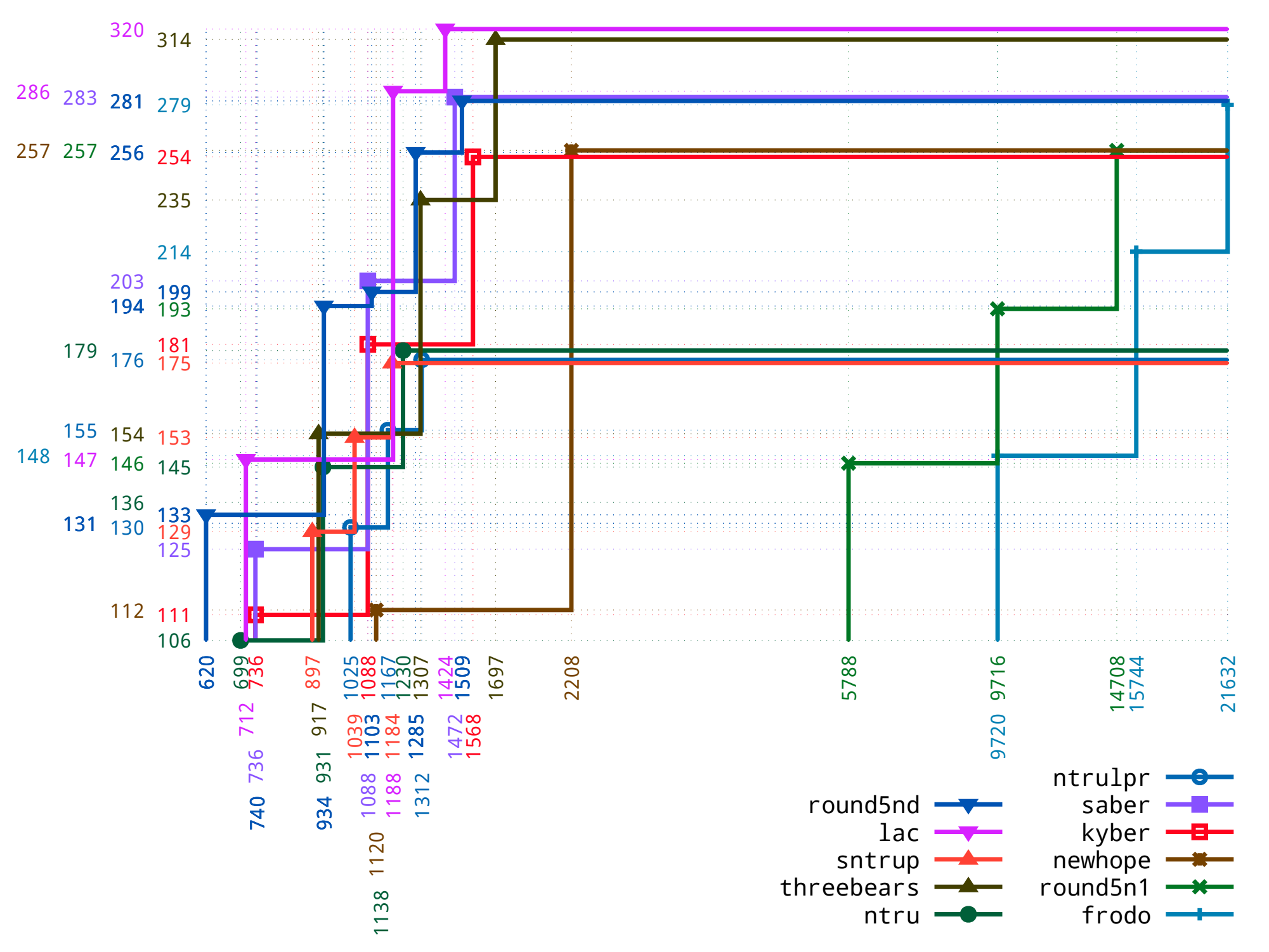
- Overstating security.
- Understating security—damaging deployment.
- Damaging comparisons: e.g. omitting "hybrid attacks"; e.g. overstating `sntrup` "rotations".

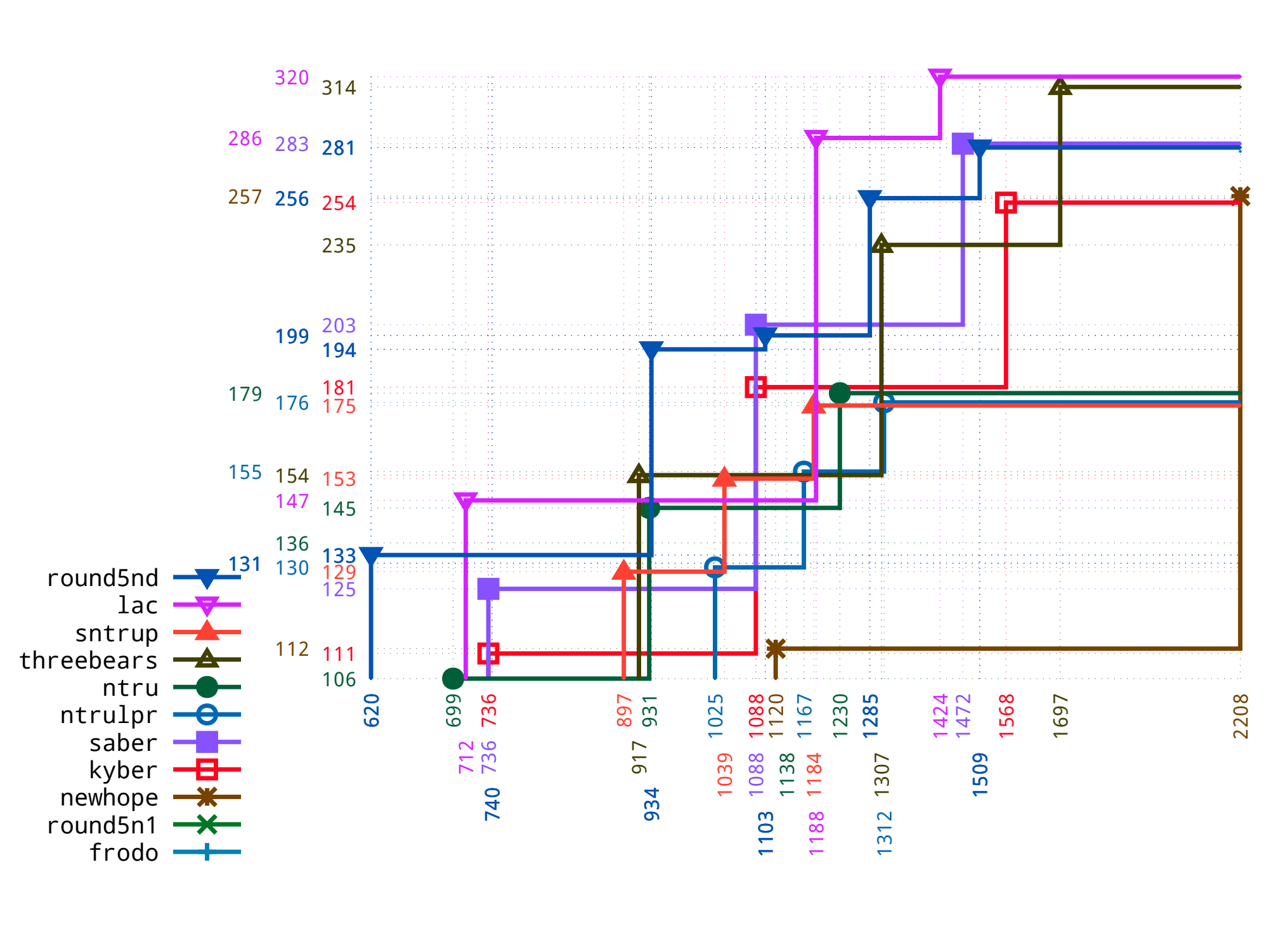
Security estimate where (claimed) data points are easiest to find: "Core-SVP" pre-quantum estimate.

Some work on better estimates; should continue this work, re-estimate all the schemes, draw new graphs.


round5nd
lac
sntrup
threebears
ntru
ntrulpr
saber
kyber
newhope
round5n1
frodo

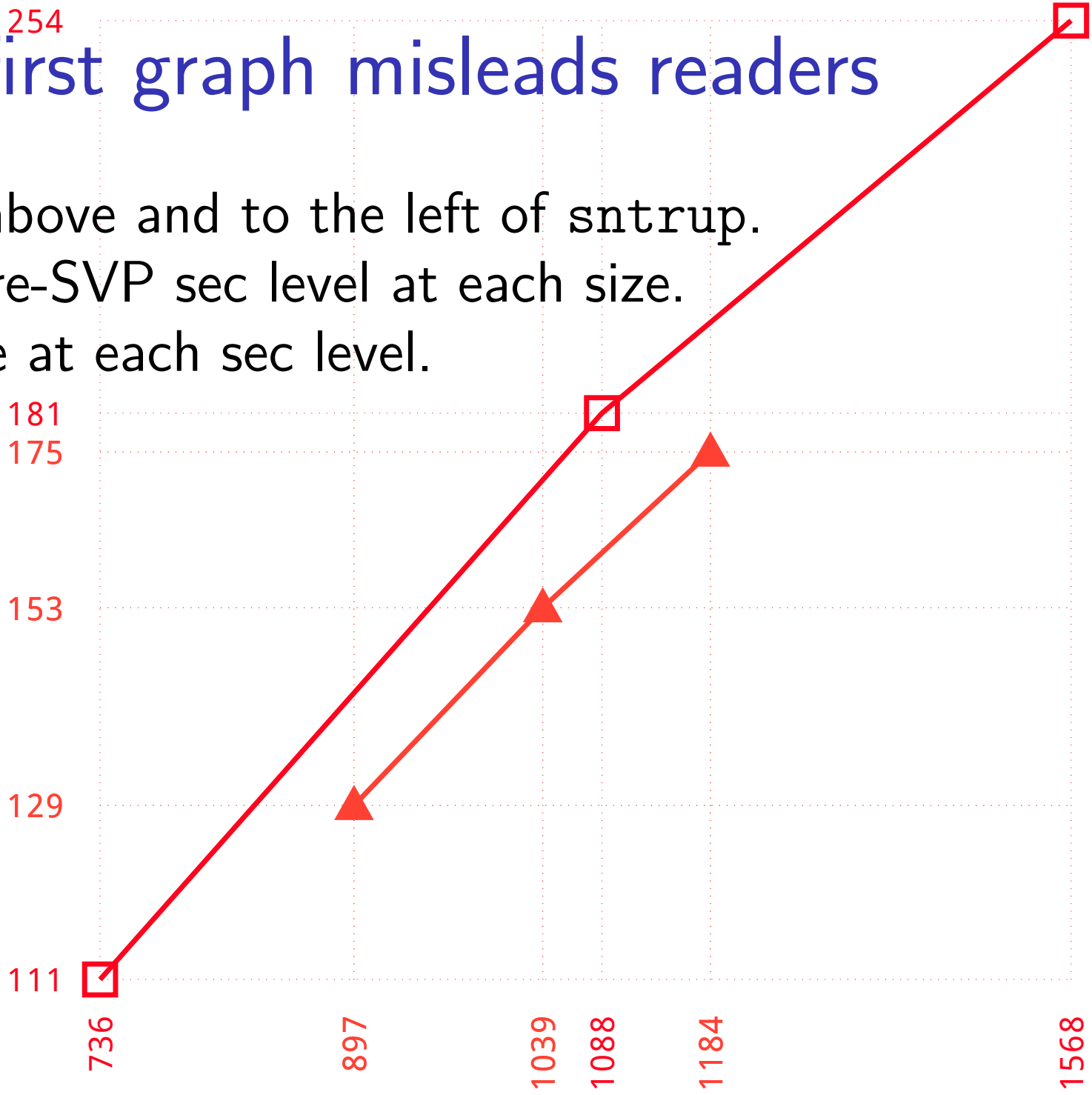

320
314
286
283
281
279
257
257
256
254
235
214
203
199
194
193
181
179
176
175
155
154
153
148
147
146
145
136
133
131
130
129
125
112
111
106
620
699
736
712
740
736
897
917
934
931
1025
1088
1039
1103
1088
1184
1188
1167
1230
1307
1285
1312
1120
1138
1424
1509
1472
1568
1697
2208
5788
9716
9720
14708
15744
21632
round5nd
lac
sntrup
threebears
ntru
ntrulpr
saber
kyber
newhope
round5n1
frodo


320
314
286
283
281
279
257
257
256
254
235
214
203
199
194
193
179
181
176
175
155
154
153
148
147
146
145
136
133
131
130
129
125
112
111
106
620
699
736
712
897
917
1025
1088
1039
1103
1167
1230
1184
1307
1285
1424
1509
1472
1568
1697
2208
5788
9716
9720
14708
15744
21632
740
736
934
931
1088
1188
1312
1120
1138
round5nd
lac
sntrup
threebears
ntru
ntrulpr
saber
kyber
newhope
round5n1
frodo


round5nd
lac
sntrup
threebears
ntru
ntrulpr
saber
kyber
newhope
round5n1
frodo
320
314
286
283
281
257
256
254
235
203
199
194
181
179
176
175
155
154
153
147
145
136
133
131
130
129
125
112
111
106
620
699
712
736
740
736
897
917
931
934
1025
1039
1088
1103
1088
1120
1138
1167
1184
1188
1230
1285
1307
1312
1424
1472
1509
1568
1697
2208

How the first graph misleads readers

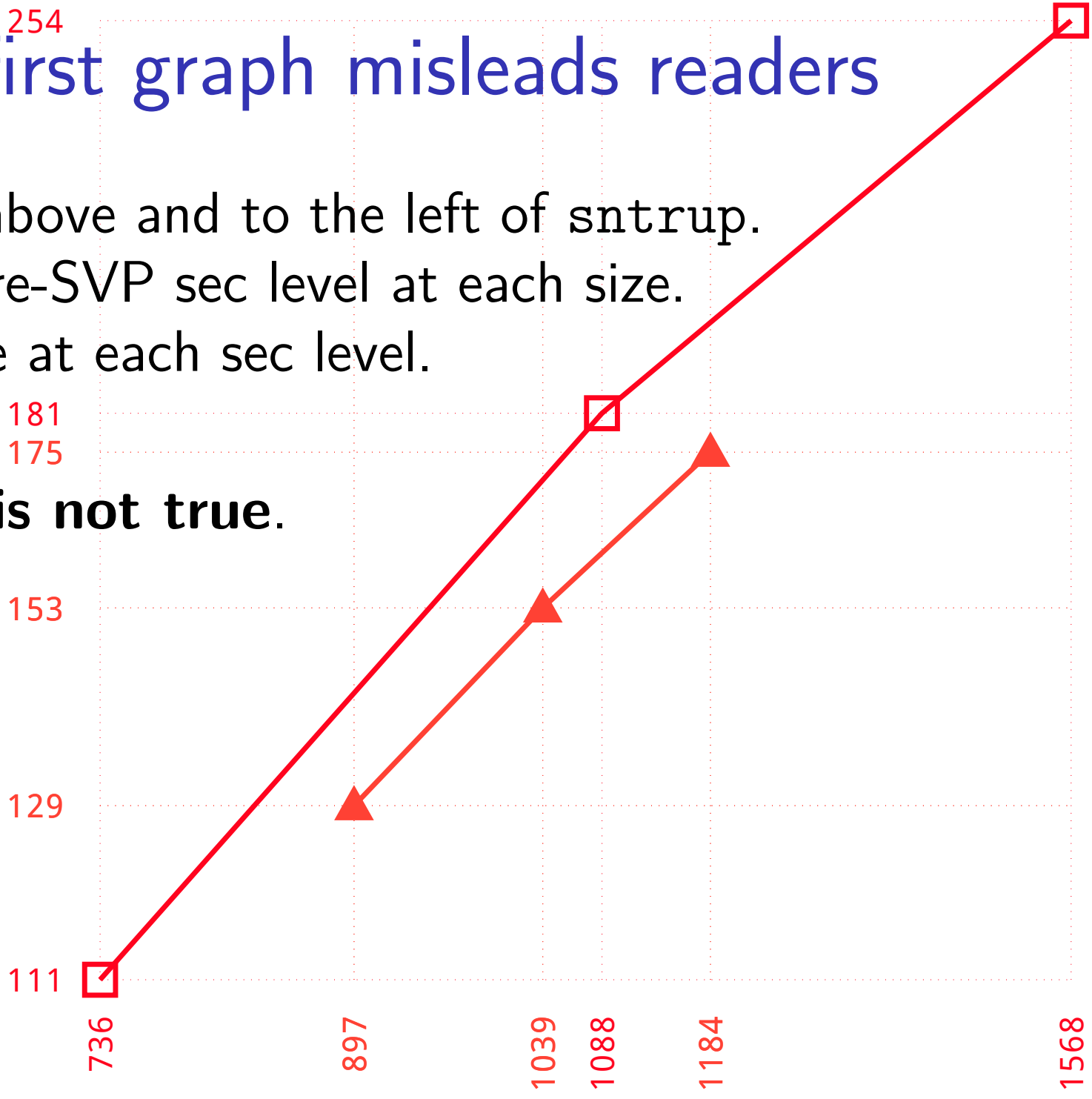
`kyber` is above and to the left of `sntrup`.
Better Core-SVP sec level at each size.
Better size at each sec level.



How the first graph misleads readers

`kyber` is above and to the left of `sntrup`.
Better Core-SVP sec level at each size.
Better size at each sec level.

But this is not true.

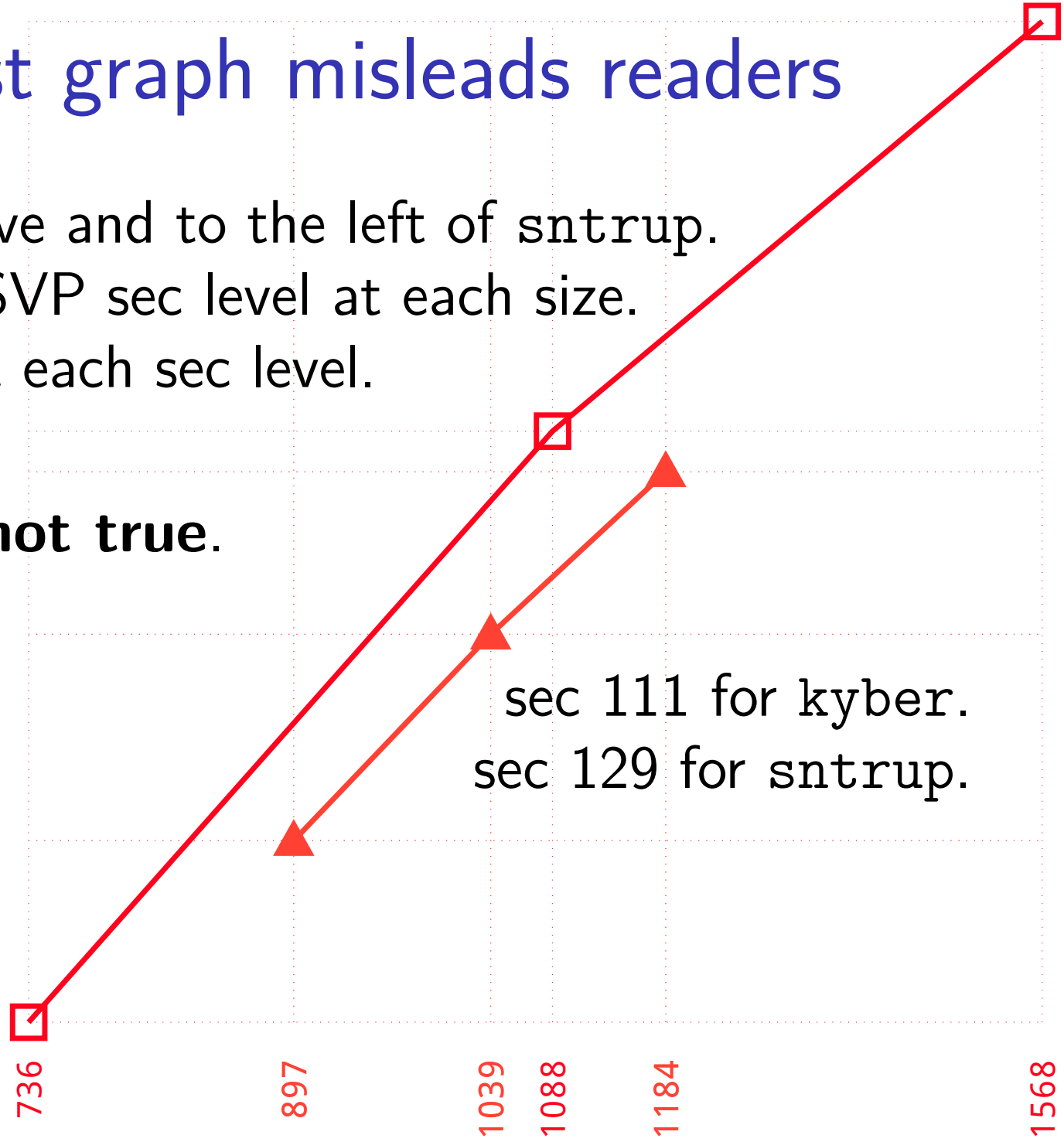


How the first graph misleads readers

`kyber` is above and to the left of `sntrup`.
Better Core-SVP sec level at each size.
Better size at each sec level.

But this is not true.

User requires size ≤ 1024:



sec 111 for `kyber`.
sec 129 for `sntrup`.

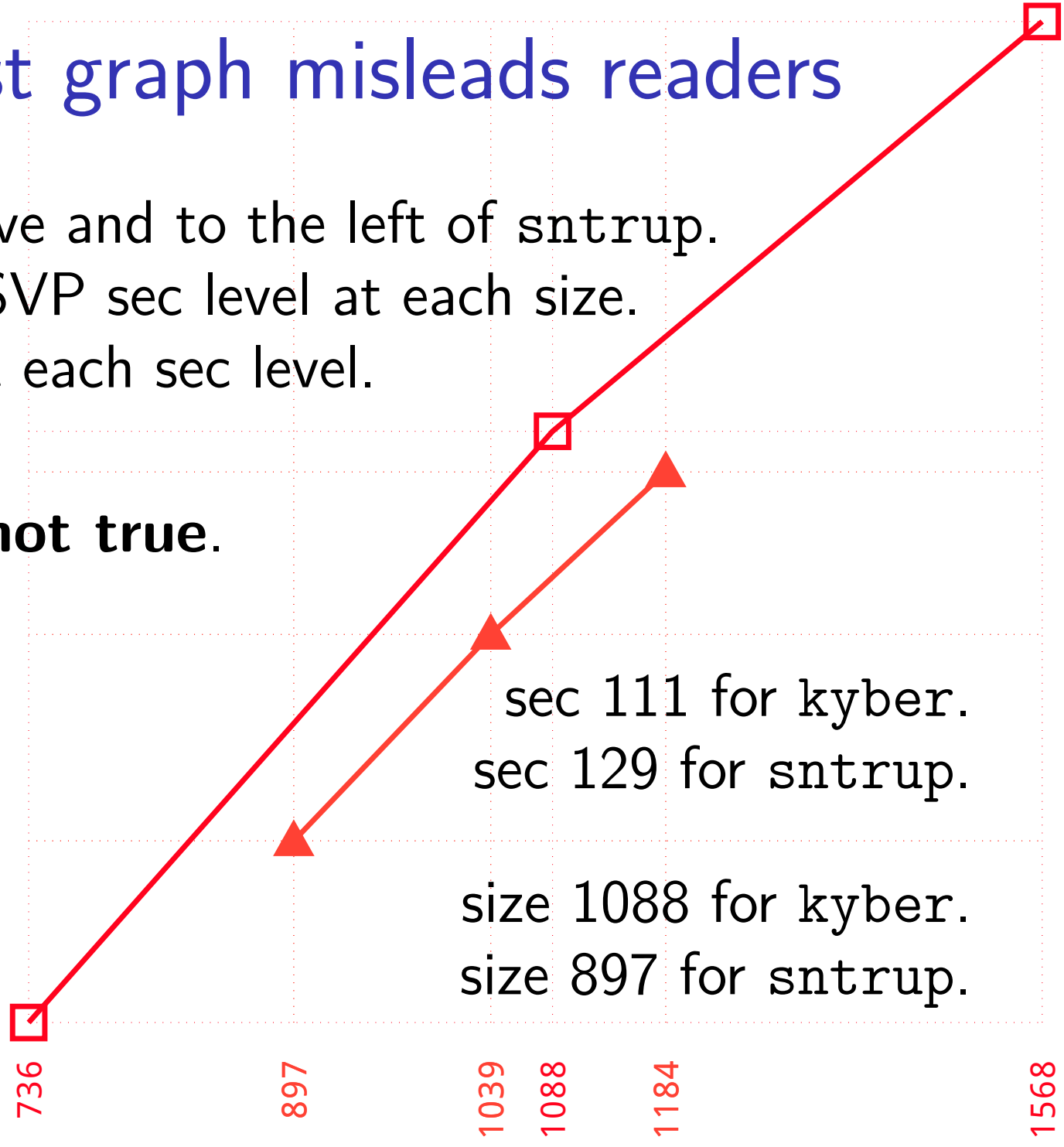
How the first graph misleads readers

`kyber` is above and to the left of `sntrup`.
Better Core-SVP sec level at each size.
Better size at each sec level.

But this is not true.

User requires size ≤ 1024:
sec 111 for `kyber`.
sec 129 for `sntrup`.

User requires sec ≥ 128:
size 1088 for `kyber`.
size 897 for `sntrup`.



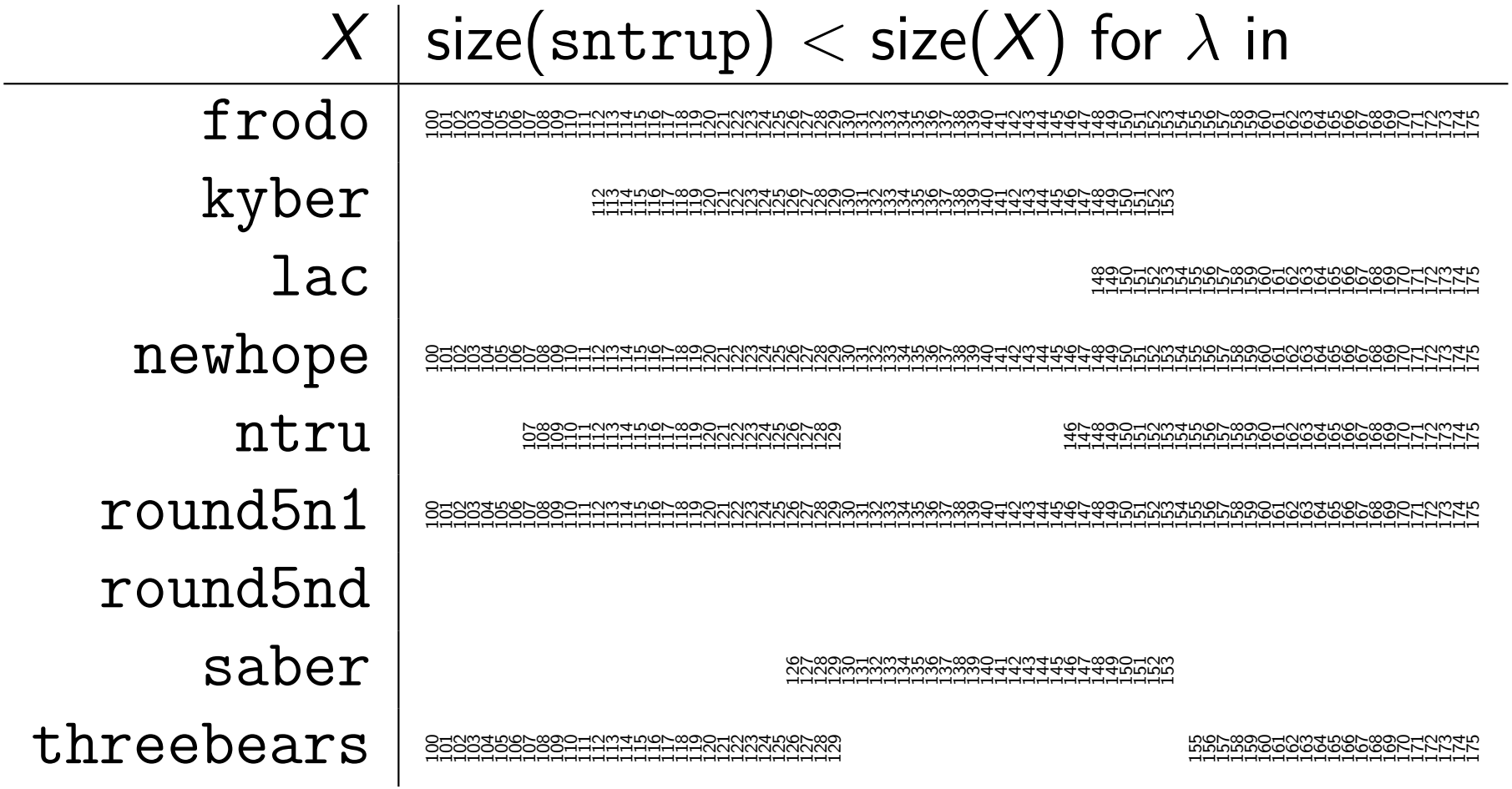
Ciphertext-size comparison examples

Core-SVP for `sntrup` options: 129, 153, 175.
User picks $\lambda \geq 100$, requires Core-SVP $\geq \lambda$.

X	size(`sntrup`) $<$ size(X) for λ in
`frodo`	$\{100, \ldots, 175\}$
`kyber`	$\{112, \ldots, 153\}$
`lac`	$\{148, \ldots, 175\}$
`newhope`	$\{100, \ldots, 175\}$
`ntru`	$\{107, \ldots, 129\} \cup \{146, \ldots, 175\}$
`round5n1`	$\{100, \ldots, 175\}$
`round5nd`	$\{\}$
`saber`	$\{126, \ldots, 153\}$
`threebears`	$\{100, \ldots, 129\} \cup \{155, \ldots, 175\}$

Ciphertext-size comparison examples

Core-SVP for `sntrup` options: 129, 153, 175.
User picks $\lambda \geq 100$, requires Core-SVP $\geq \lambda$.



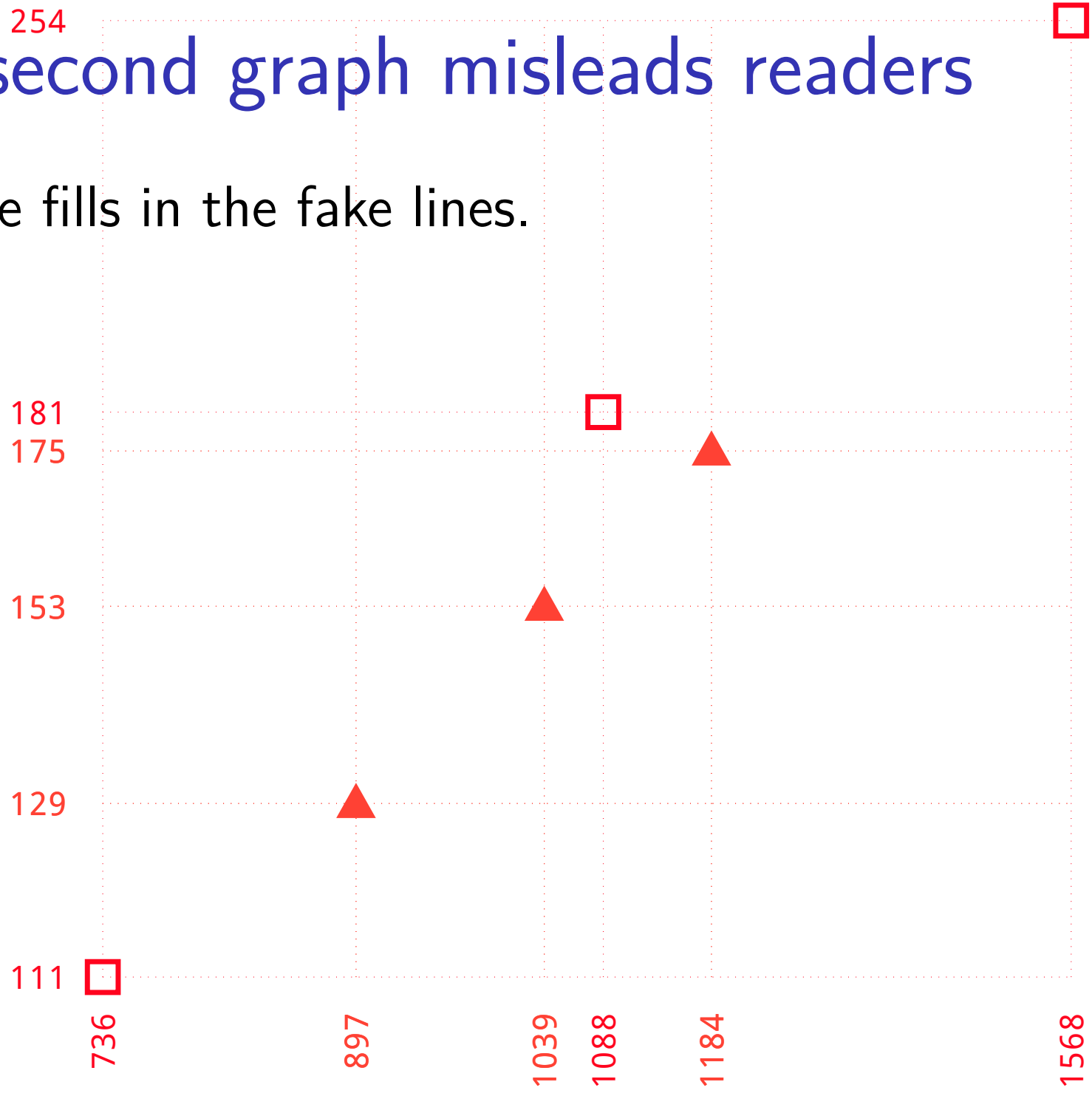
Core-SVP comparison examples

Ciphertext sizes for `sntrup`: 897, 1039, 1184.
User picks $S \leq 1280$, requires ciphertext size $\leq S$.

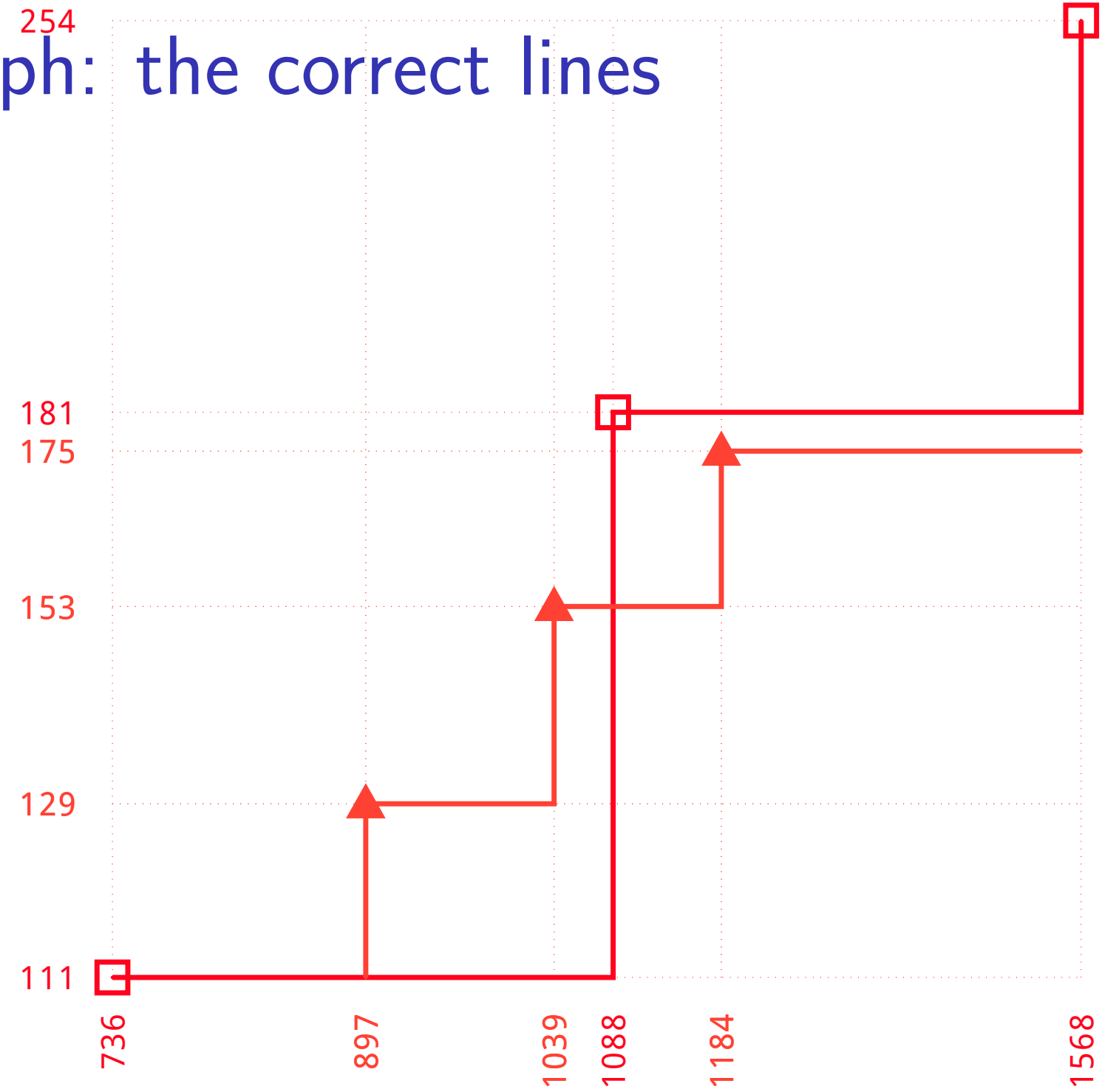
X	$\mathsf{sec}(\texttt{sntrup}) > \mathsf{sec}(X)$ for S in
`frodo`	$\{897, \ldots, 1280\}$
`kyber`	$\{897, \ldots, 1087\}$
`lac`	$\{1039, \ldots, 1187\}$
`newhope`	$\{897, \ldots, 1280\}$
`ntru`	$\{897, \ldots, 930\} \cup \{1039, \ldots, 1229\}$
`round5n1`	$\{897, \ldots, 1280\}$
`round5nd`	$\{\}$
`saber`	$\{897, \ldots, 1087\}$
`threebears`	$\{897, \ldots, 916\} \cup \{1184, \ldots, 1280\}$

How the second graph misleads readers

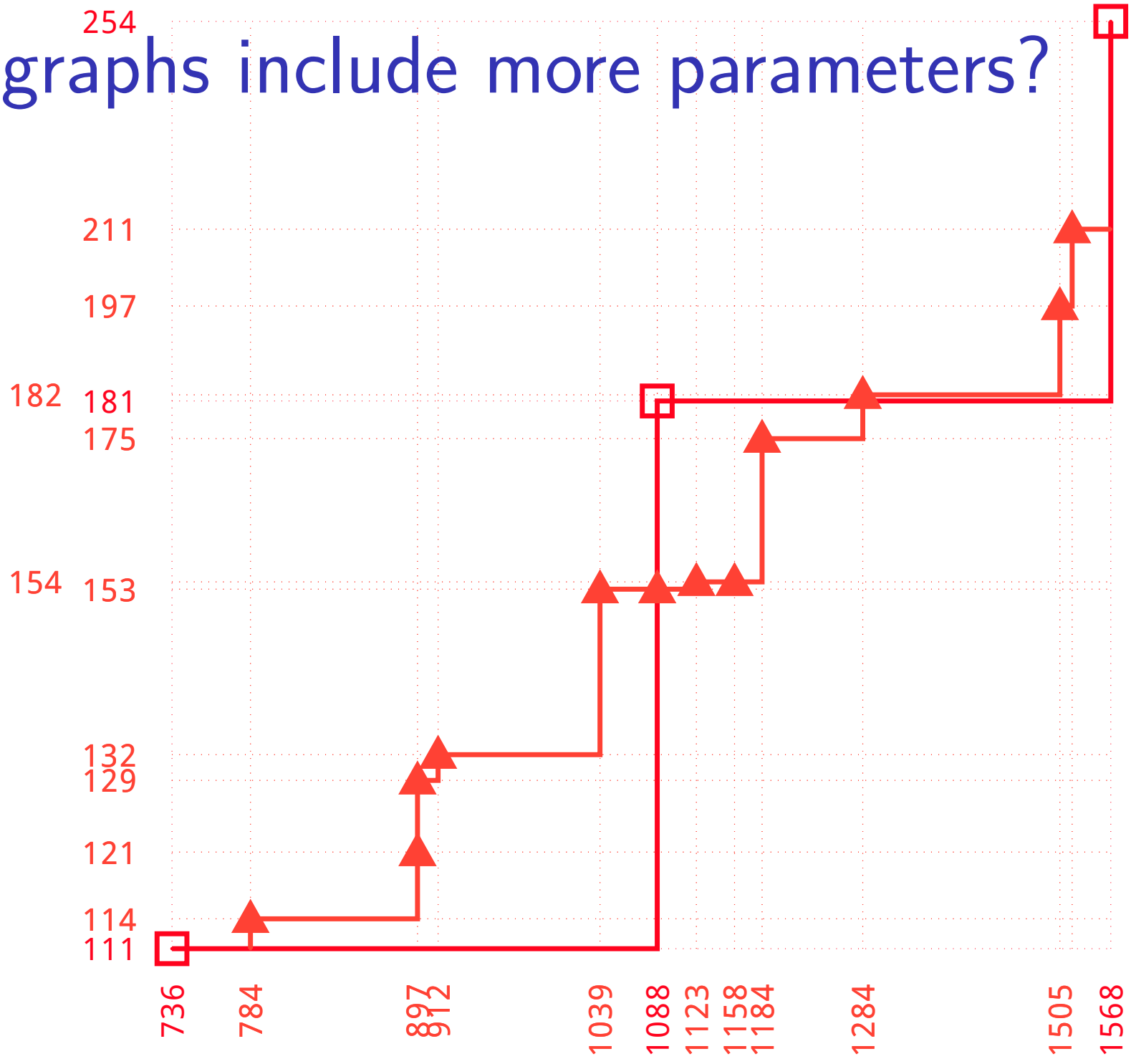
Human eye fills in the fake lines.



Third graph: the correct lines



Should graphs include more parameters?



Should graphs include more parameters?