

**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. `ntrup` beats `sntrup` in key size,

but `sntrup` beats `ntrup` 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. `ntrup` beats `sntrup` in key size,
but `sntrup` beats `ntrup` 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 `snttrup` “rotations”.

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

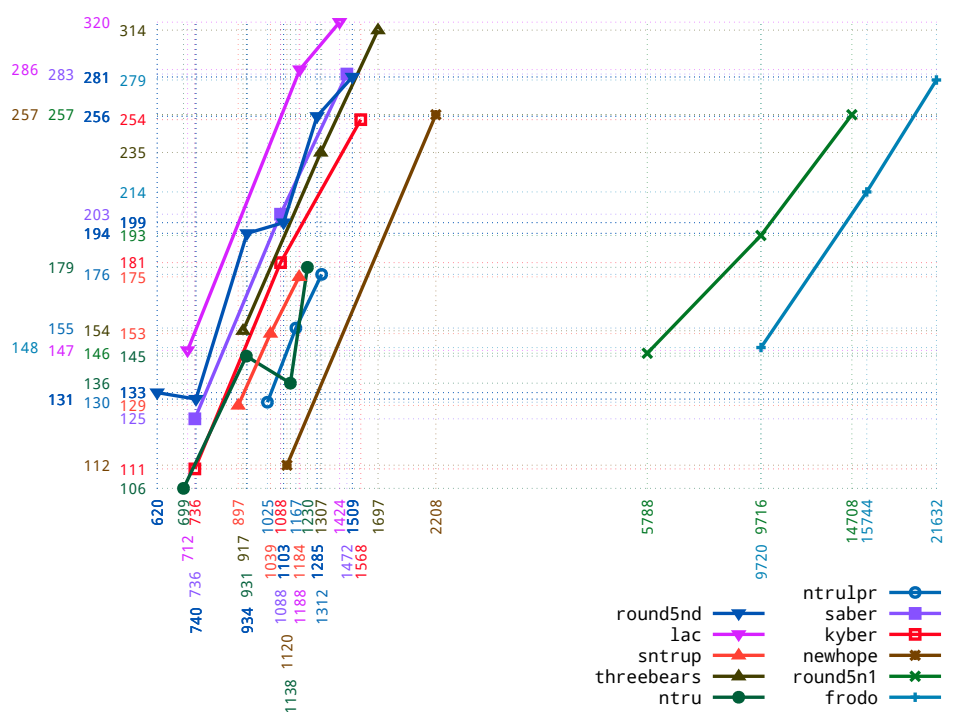
Vertical axis: Core-SVP security estimate

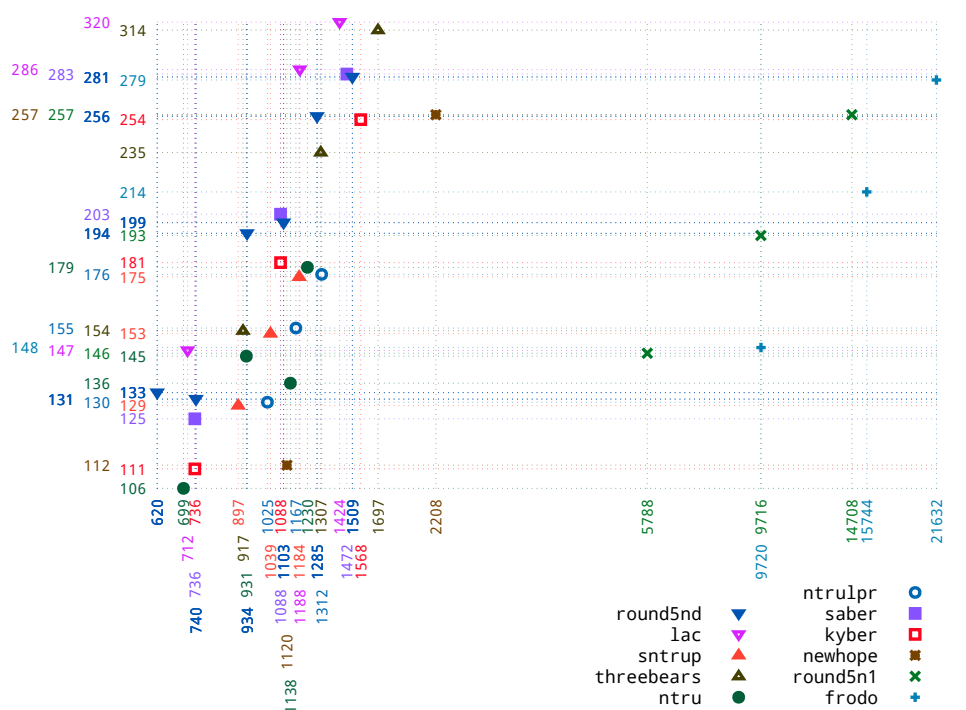
Beware (potential/actual) oversimplifications inside lattice security estimates. Can lead to:

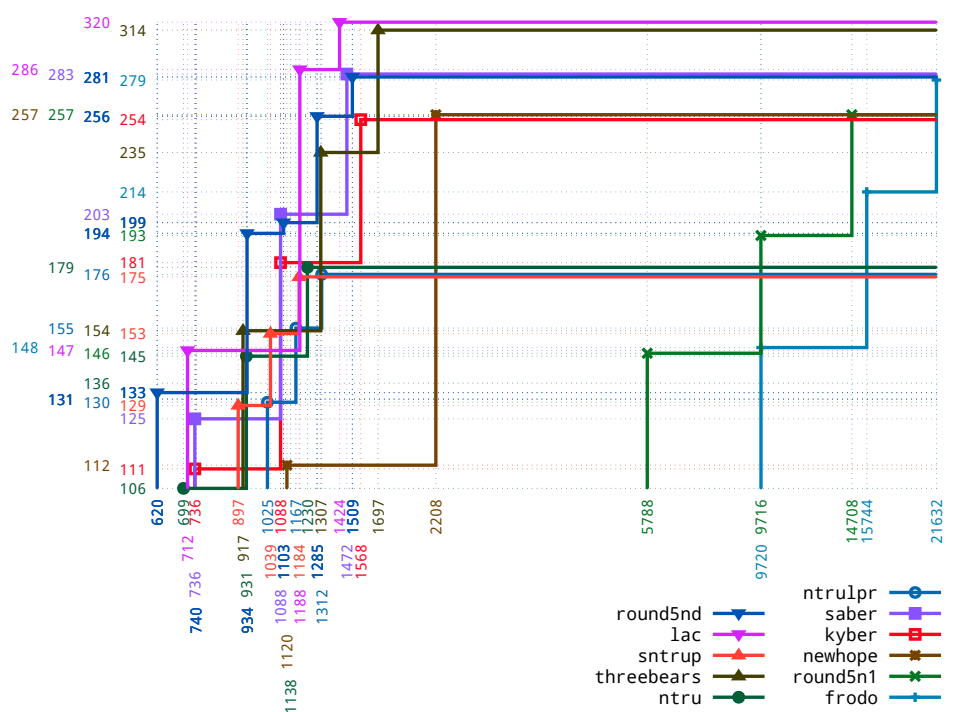
- Overstating security.
- Understating security—damaging deployment.
- Damaging comparisons: e.g. omitting “hybrid attacks”; e.g. overstating `snttrup` “rotations”.

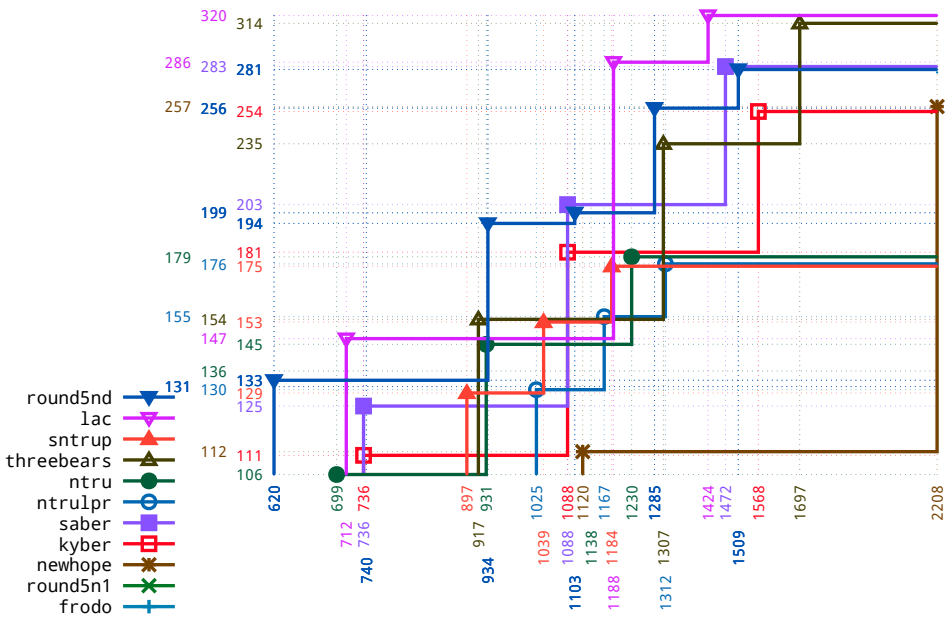
Security estimate where (claimed) data points are easiest to find: “Core-SVP” pre-quantum estimate.

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



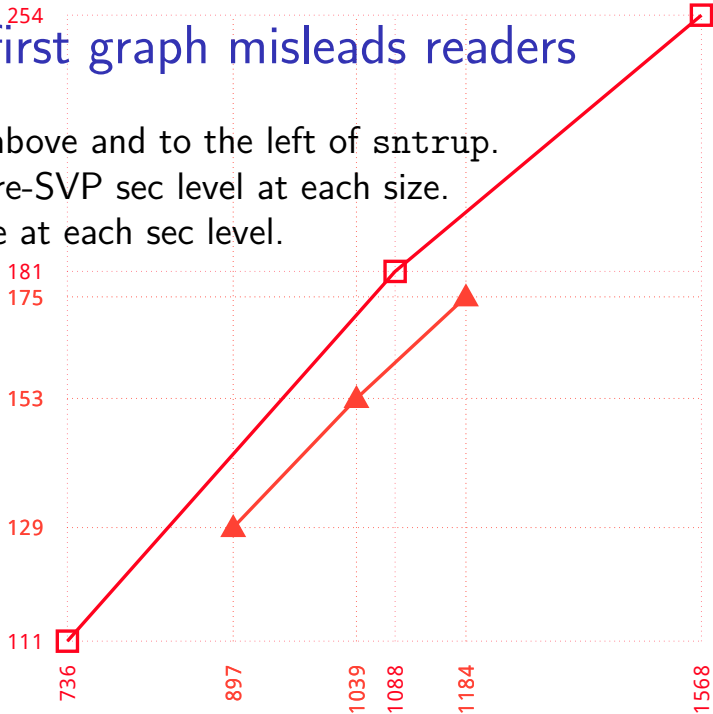






How the first graph misleads readers

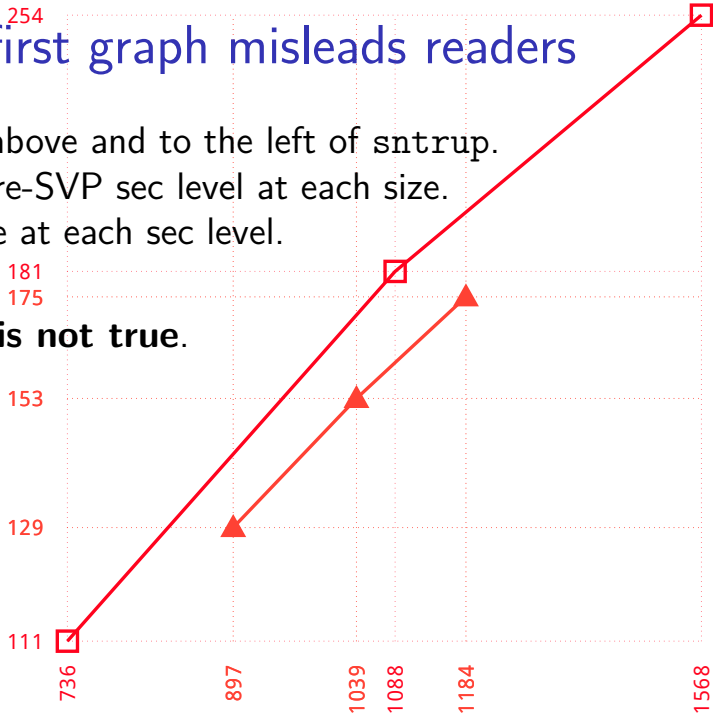
kyber is above and to the left of sntrup.
Better Core-SVP sec level at each size.
Better size at each sec level.



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.



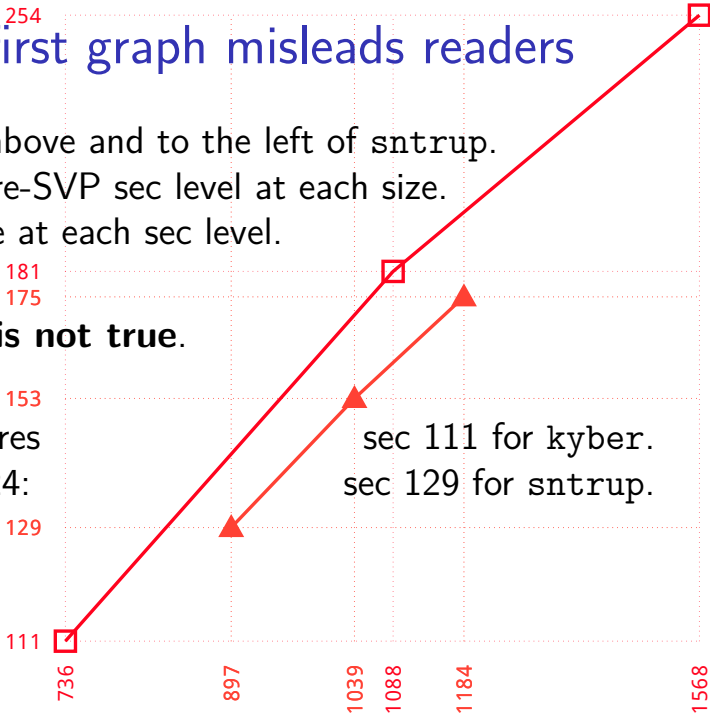
How the first graph misleads readers

kyber is above and to the left of snttrup.
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 snttrup.



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.

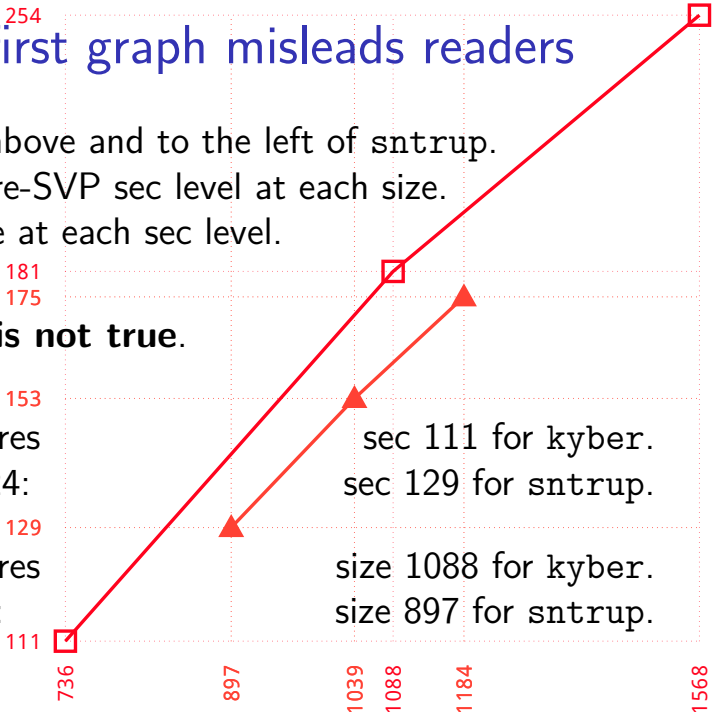
But this is not true.

User requires
size ≤ 1024 :

User requires
sec ≥ 128 :

sec 111 for kyber.
sec 129 for sntrup.

size 1088 for kyber.
size 897 for sntrup.



Ciphertext-size comparison examples

Core-SVP for sntrup options: 129, 153, 175.


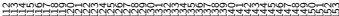

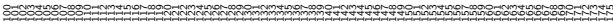





User picks $\lambda \geq 100$, requires Core-SVP $\geq \lambda$.

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

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	
kyber	
lac	
newhope	
ntru	
round5n1	
round5nd	
saber	
threebears	

Core-SVP comparison examples

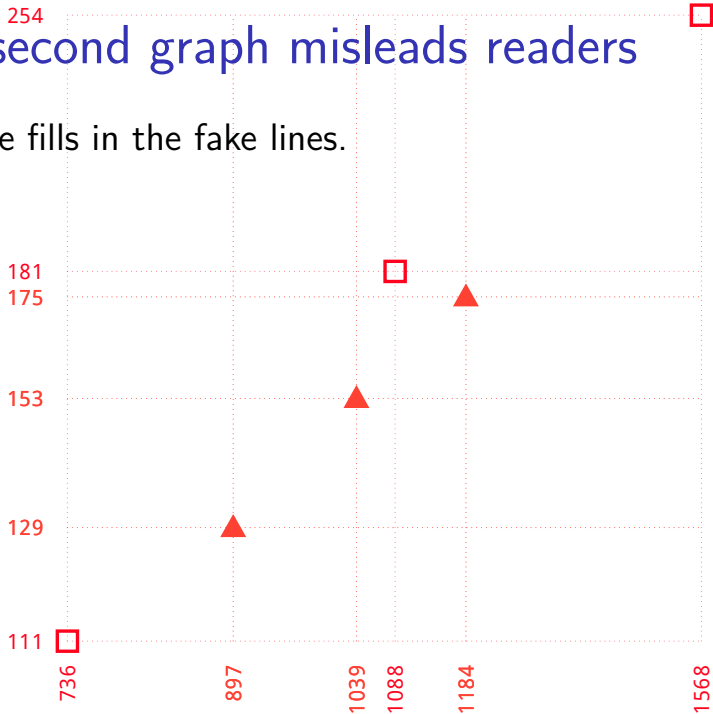
Ciphertext sizes for sntrup: 897, 1039, 1184.

User picks $S \leq 1280$, requires ciphertext size $\leq S$.

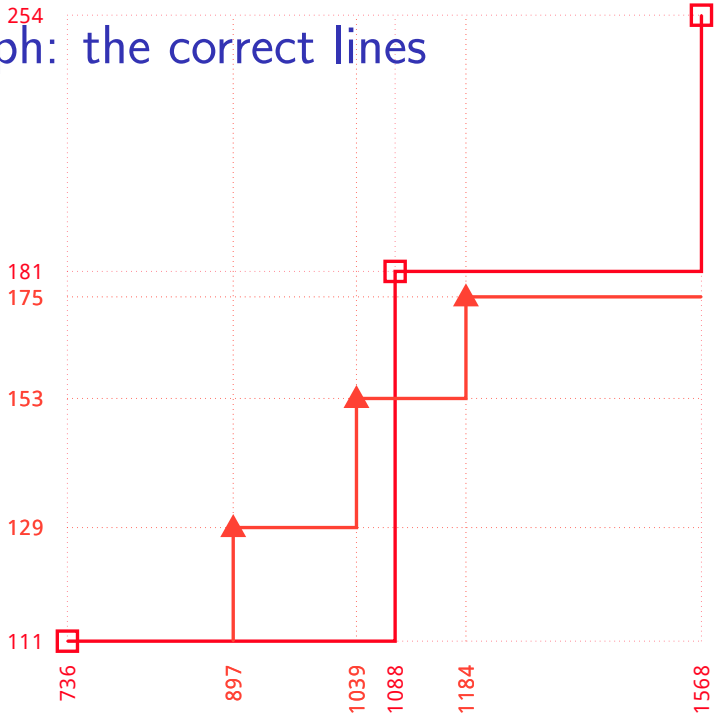
X	$\text{sec}(\text{sntrup}) > \text{sec}(X)$ for S in
frodo	$\{897, \dots, 1280\}$
kyber	$\{897, \dots, 1087\}$
lac	$\{1039, \dots, 1187\}$
newhope	$\{897, \dots, 1280\}$
ntru	$\{897, \dots, 930\} \cup \{1039, \dots, 1229\}$
round5n1	$\{897, \dots, 1280\}$
round5nd	$\{\}$
saber	$\{897, \dots, 1087\}$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

How the second graph misleads readers

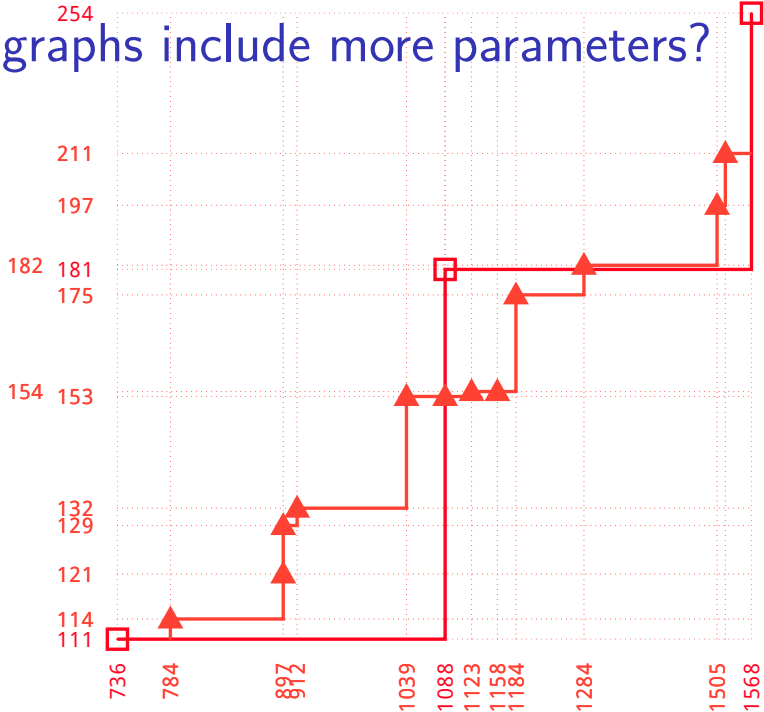
Human eye fills in the fake lines.



Third graph: the correct lines



Should graphs include more parameters?



Should graphs include more parameters?

