

Biclique Cryptanalysis of the Full AES

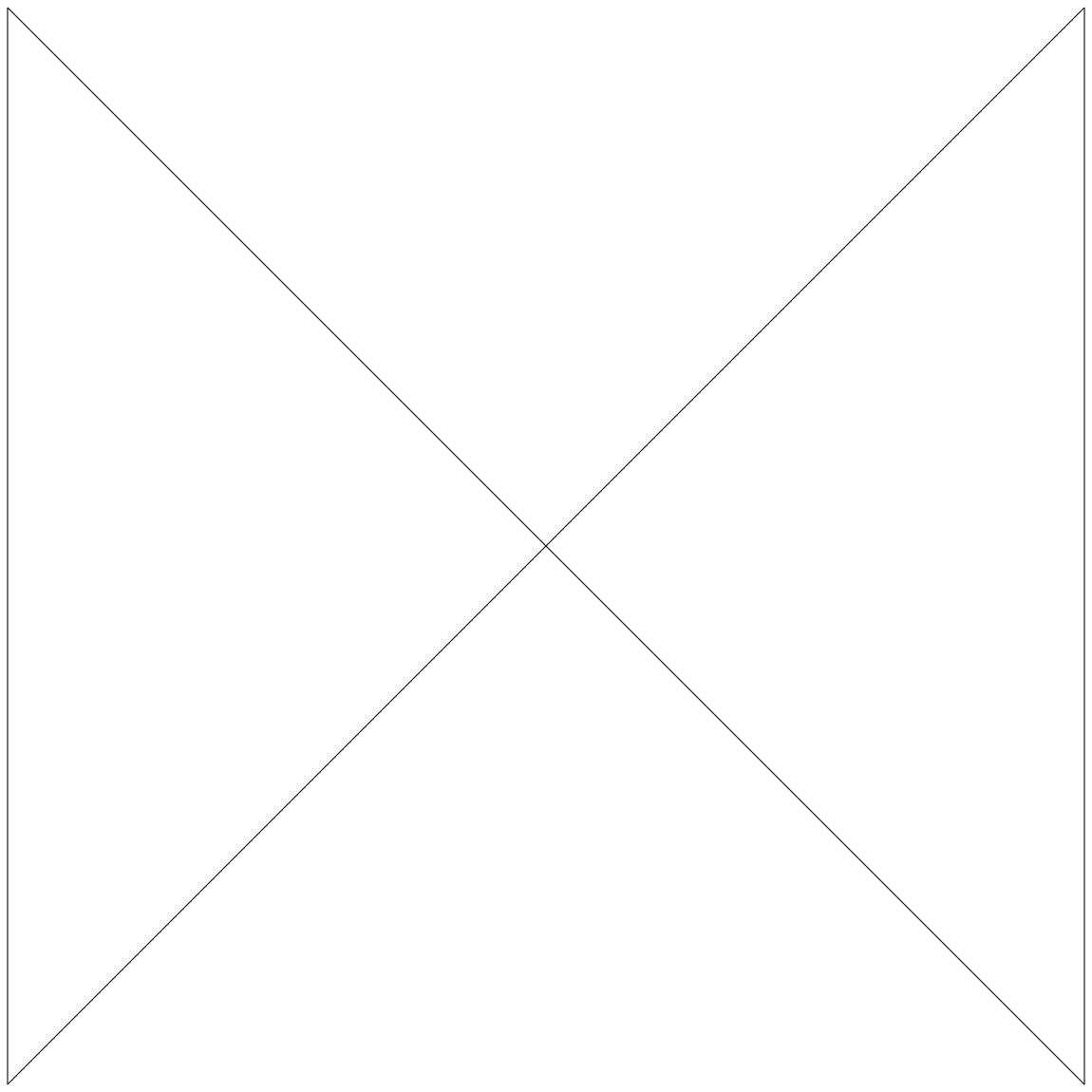
Andrey Bogdanov, Dmitry Khovratovich, Christian Rechberger

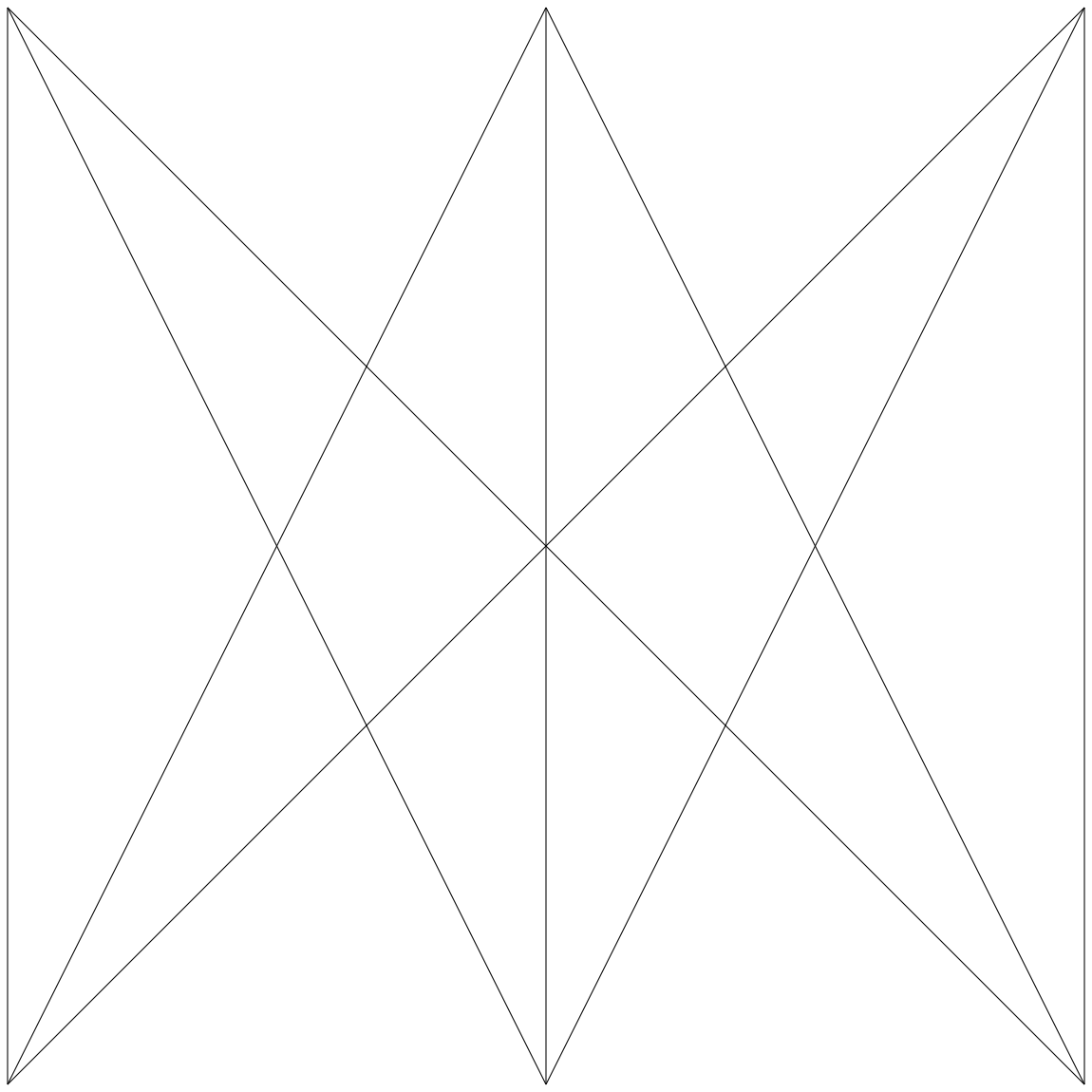
Microsoft Research - KU Leuven - ENS

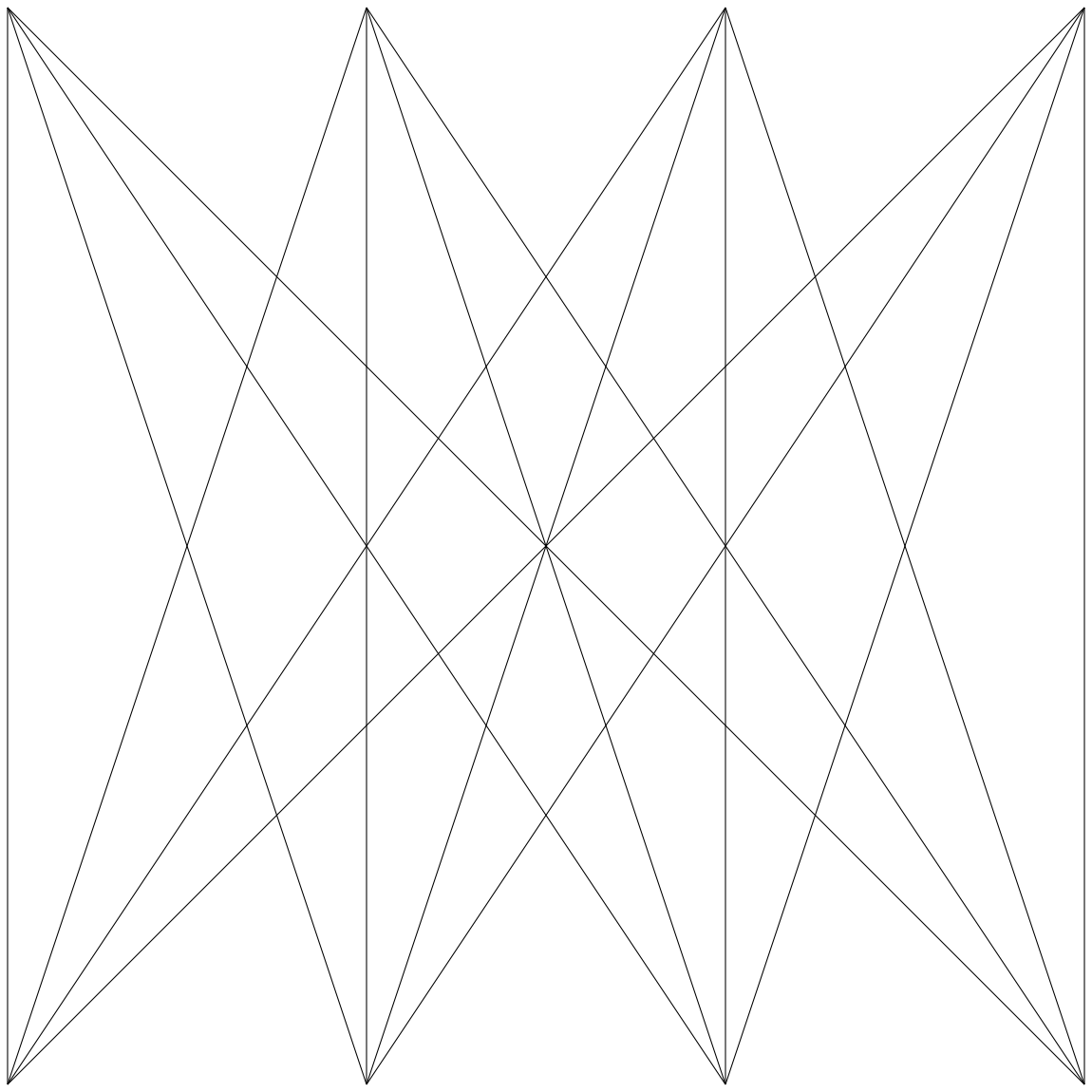
16 August 2011

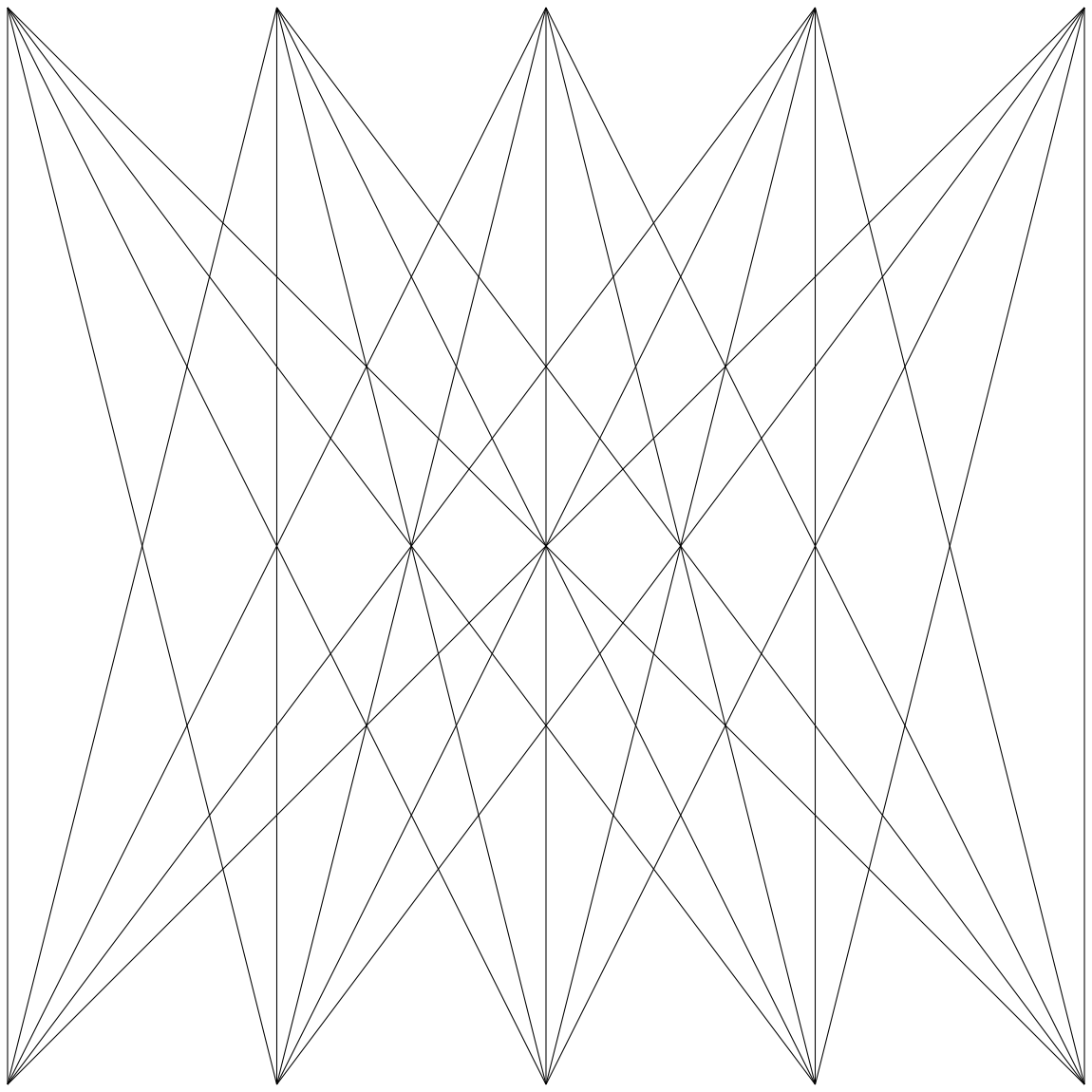
Or:
Why you might want to rename
AES-128 into AES-126
in a few minutes

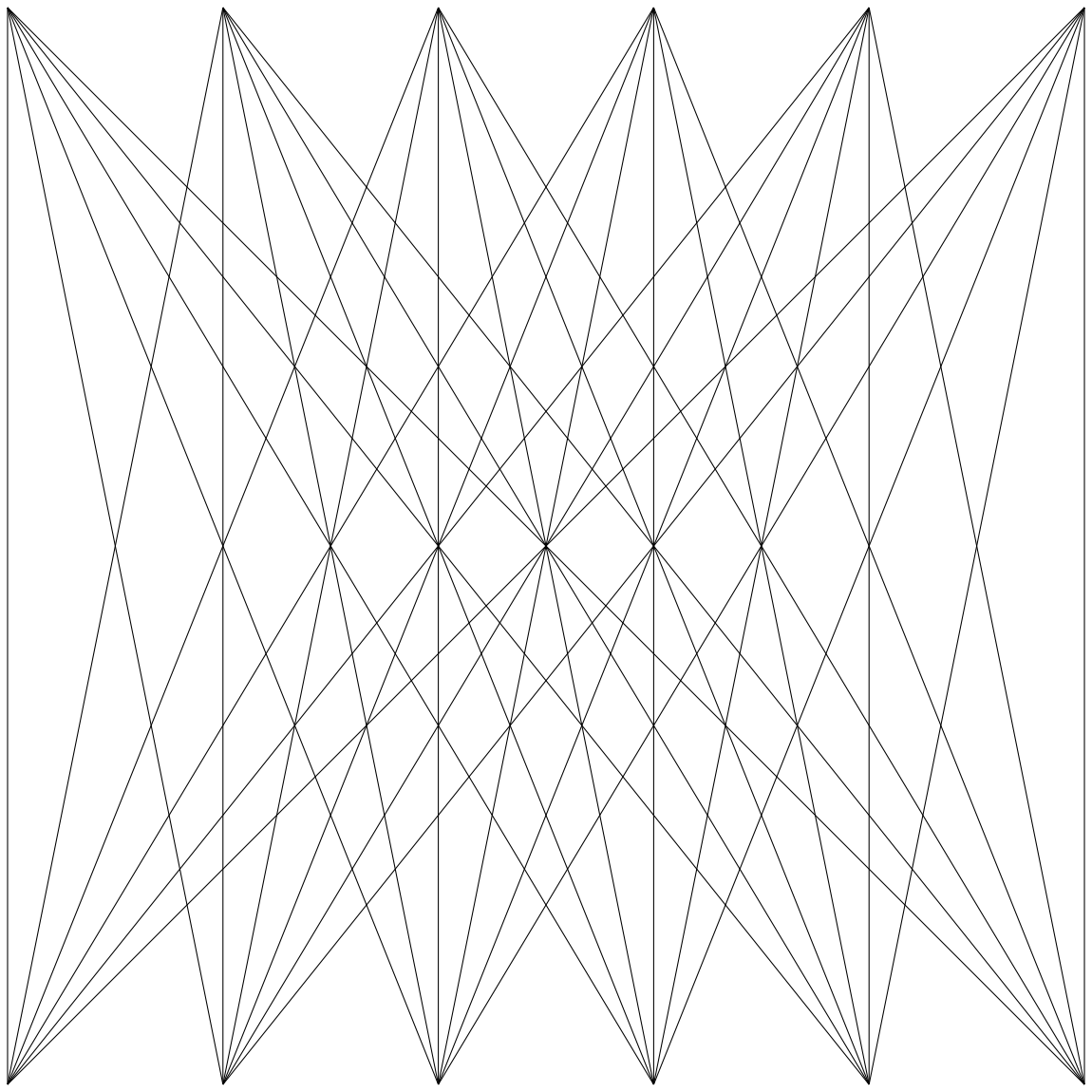
Biclique?

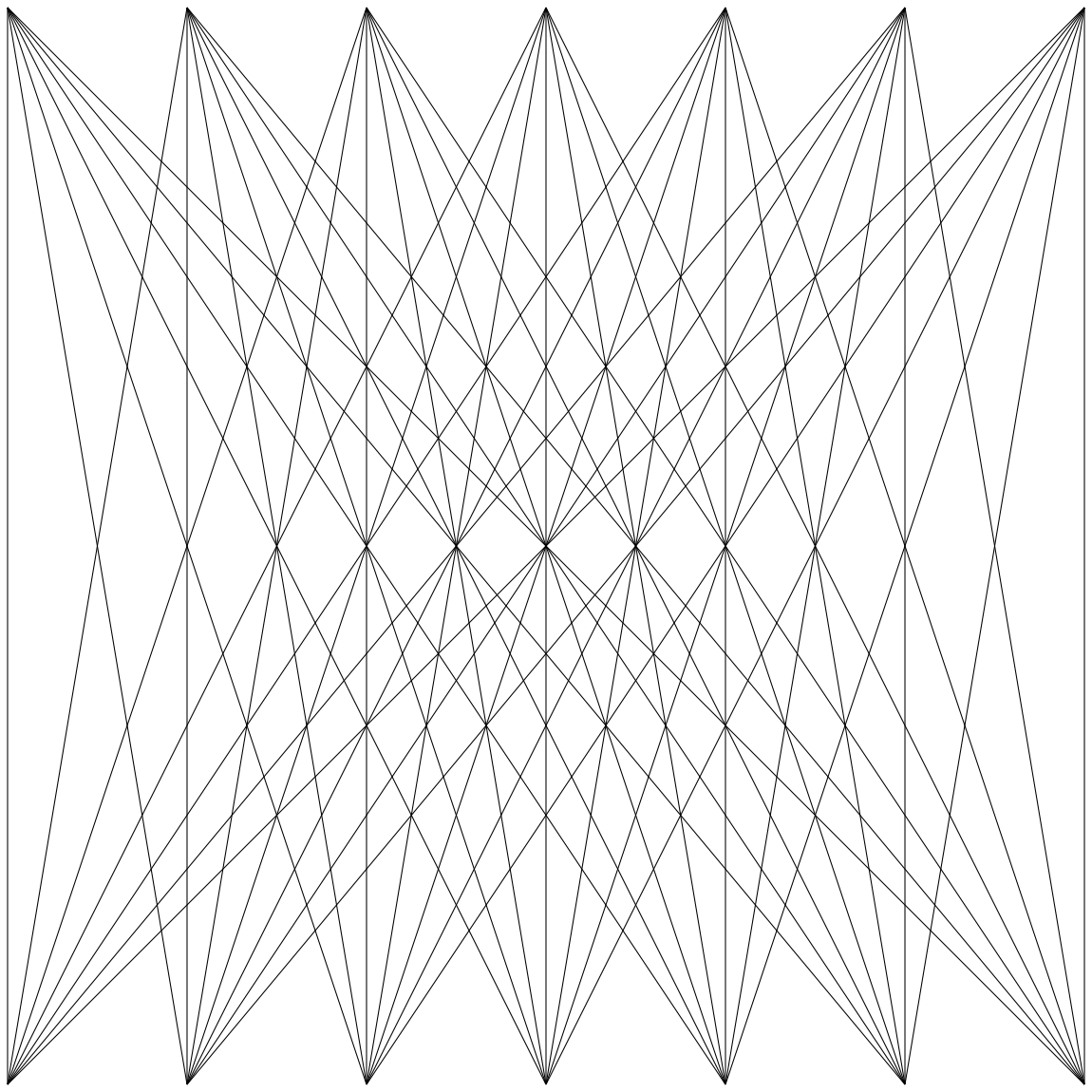


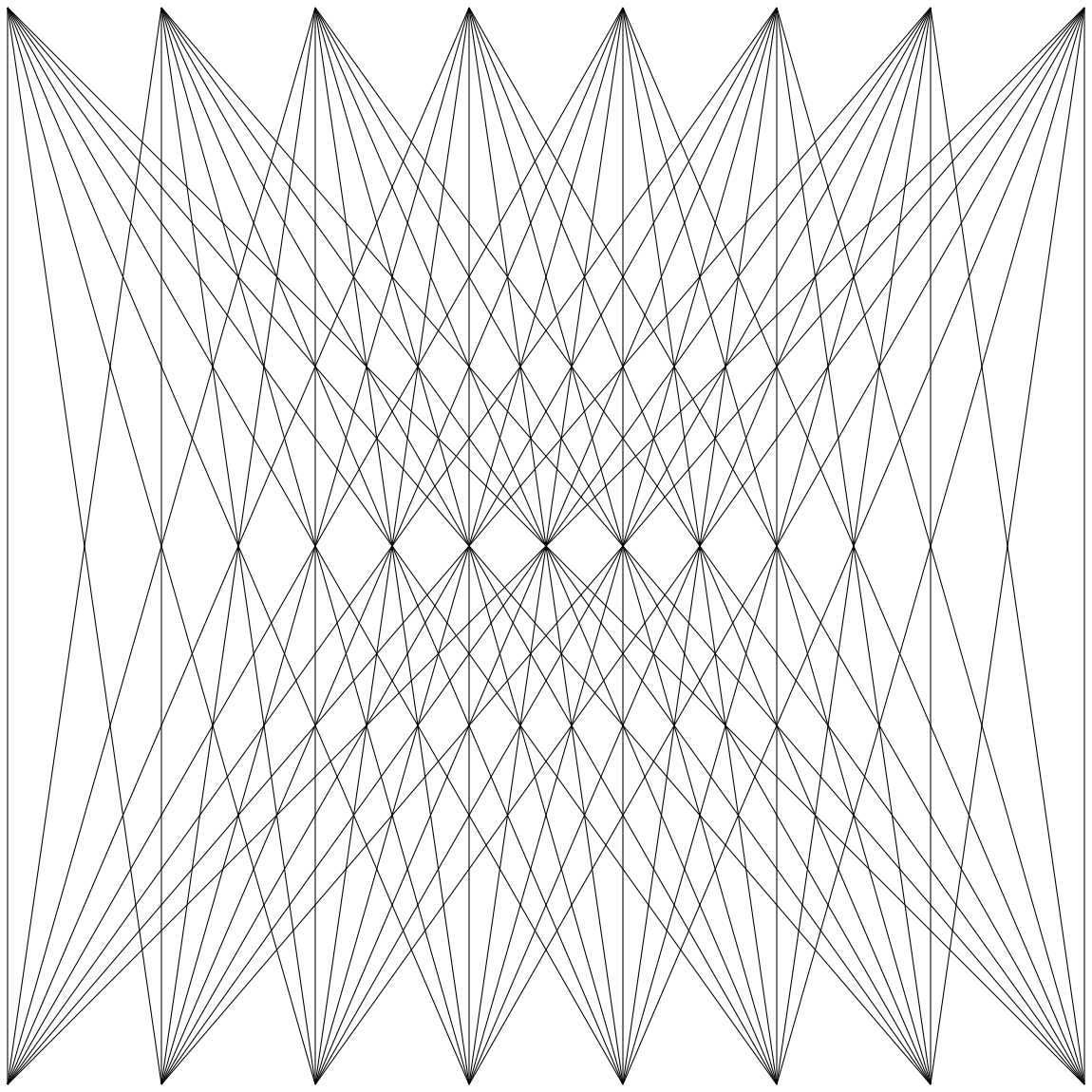


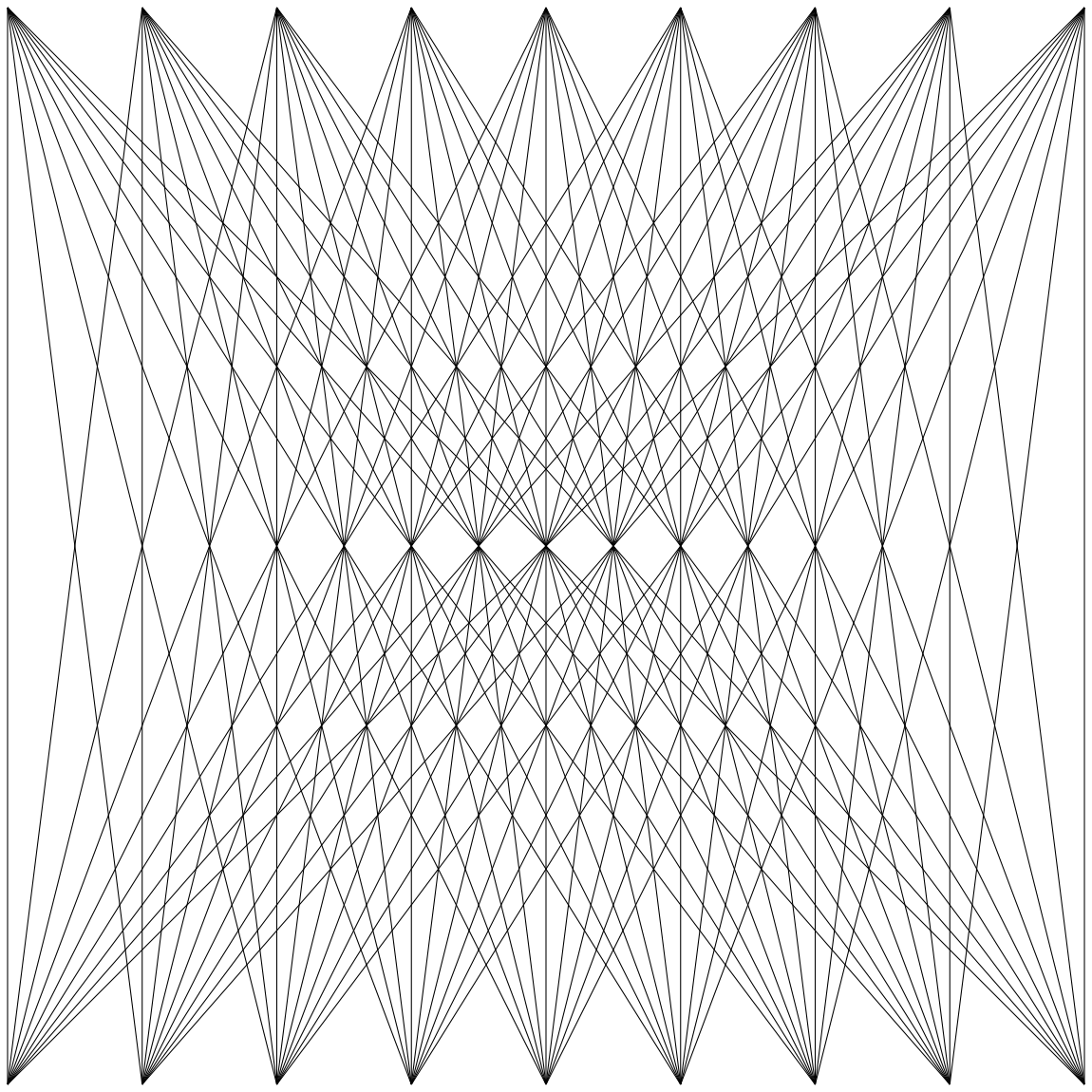


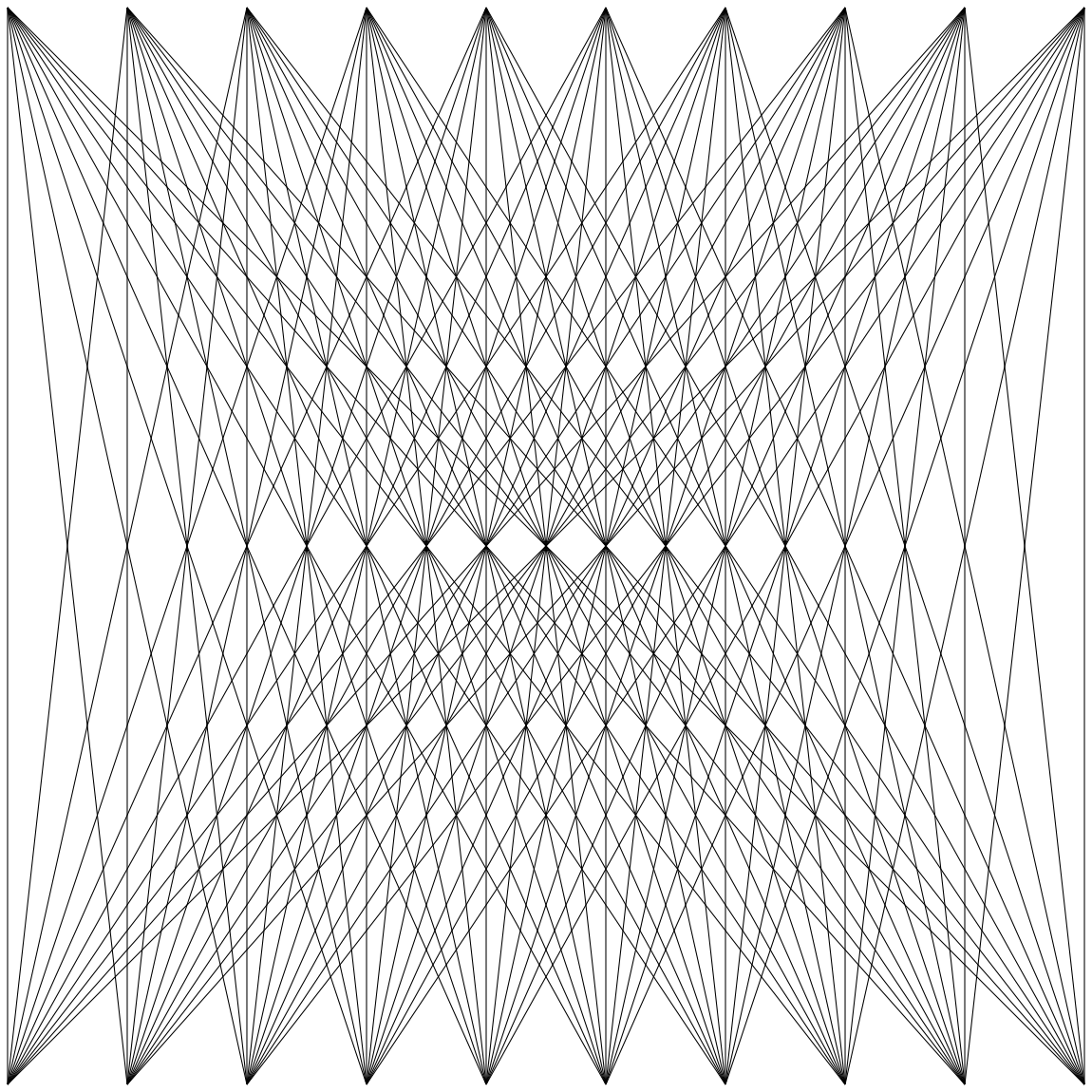


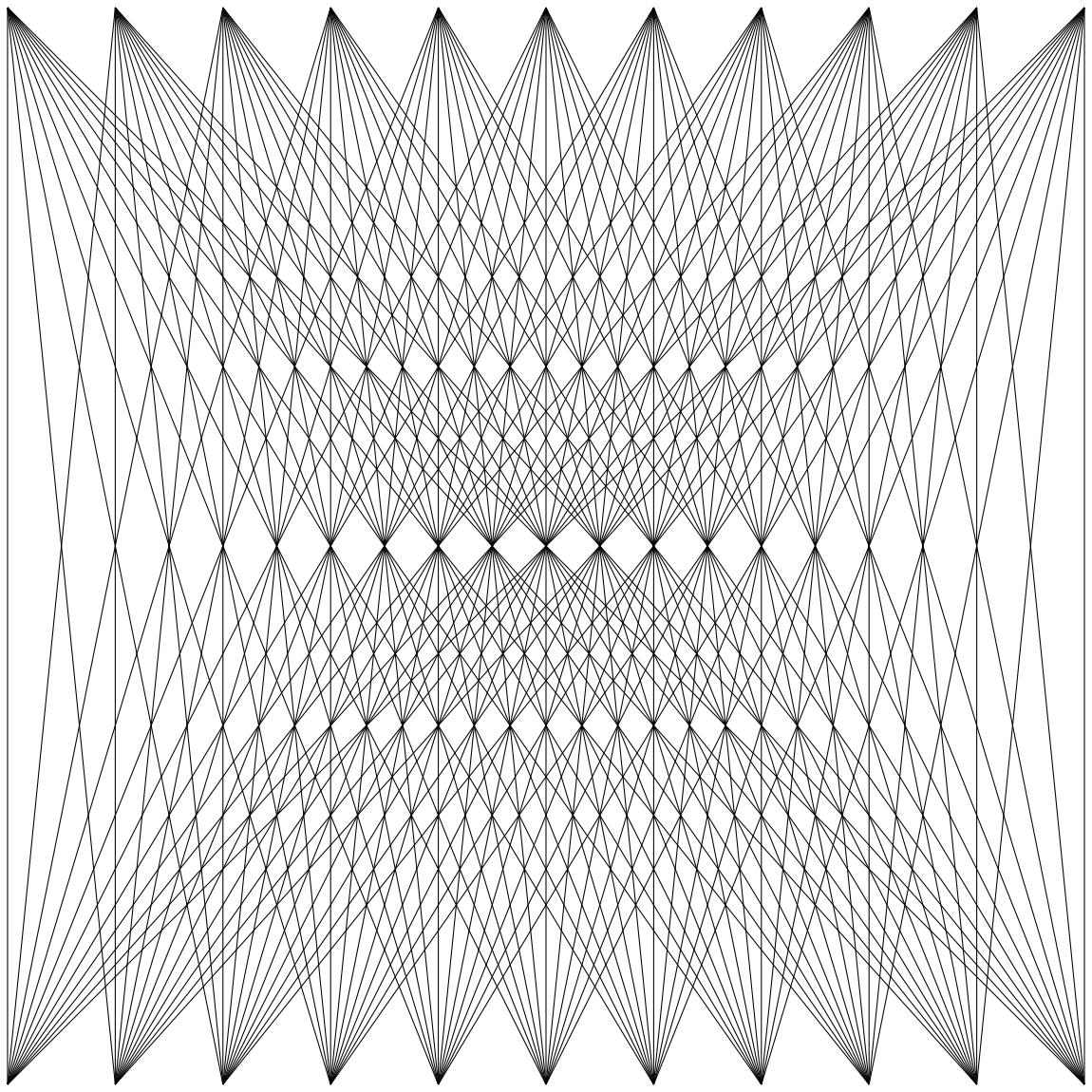


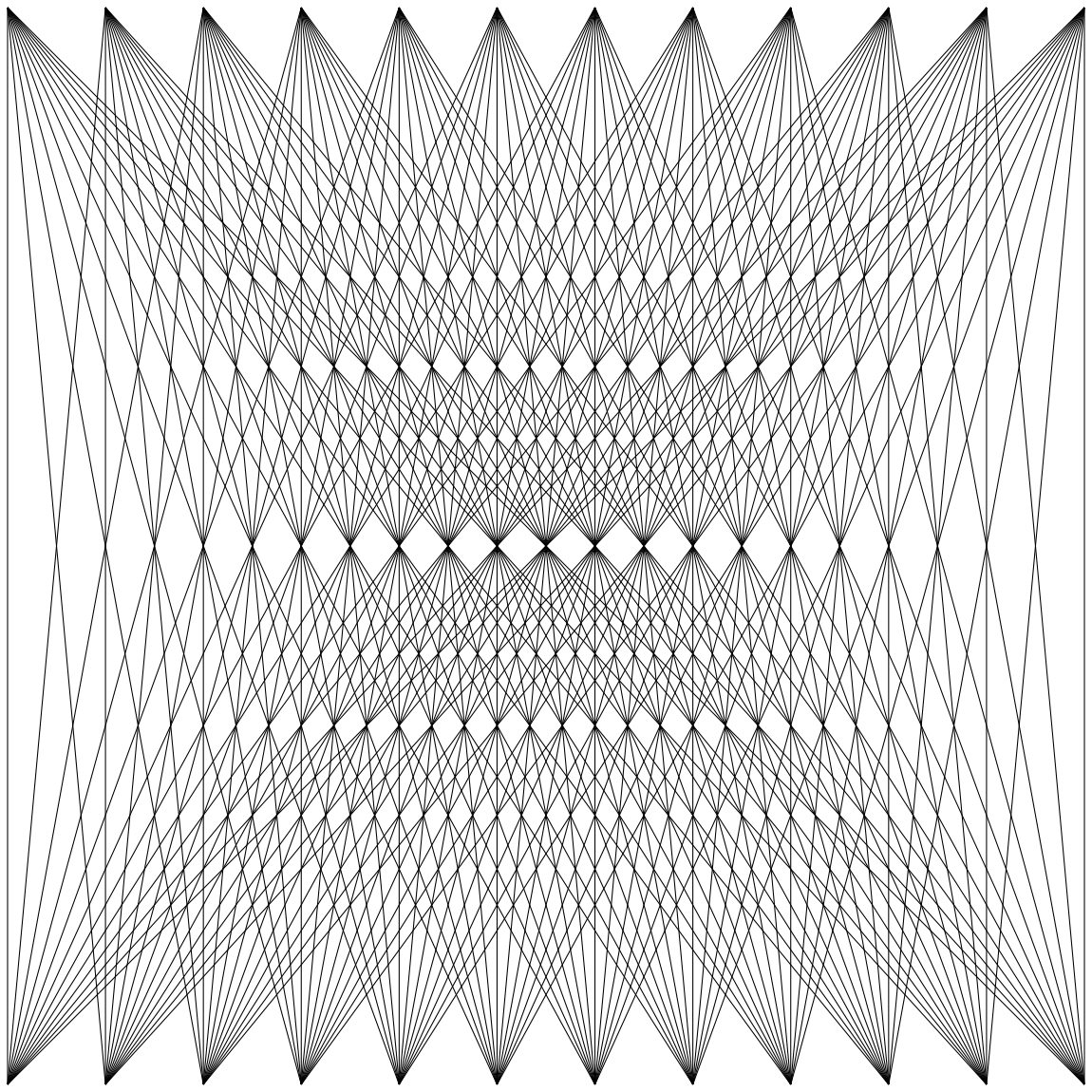


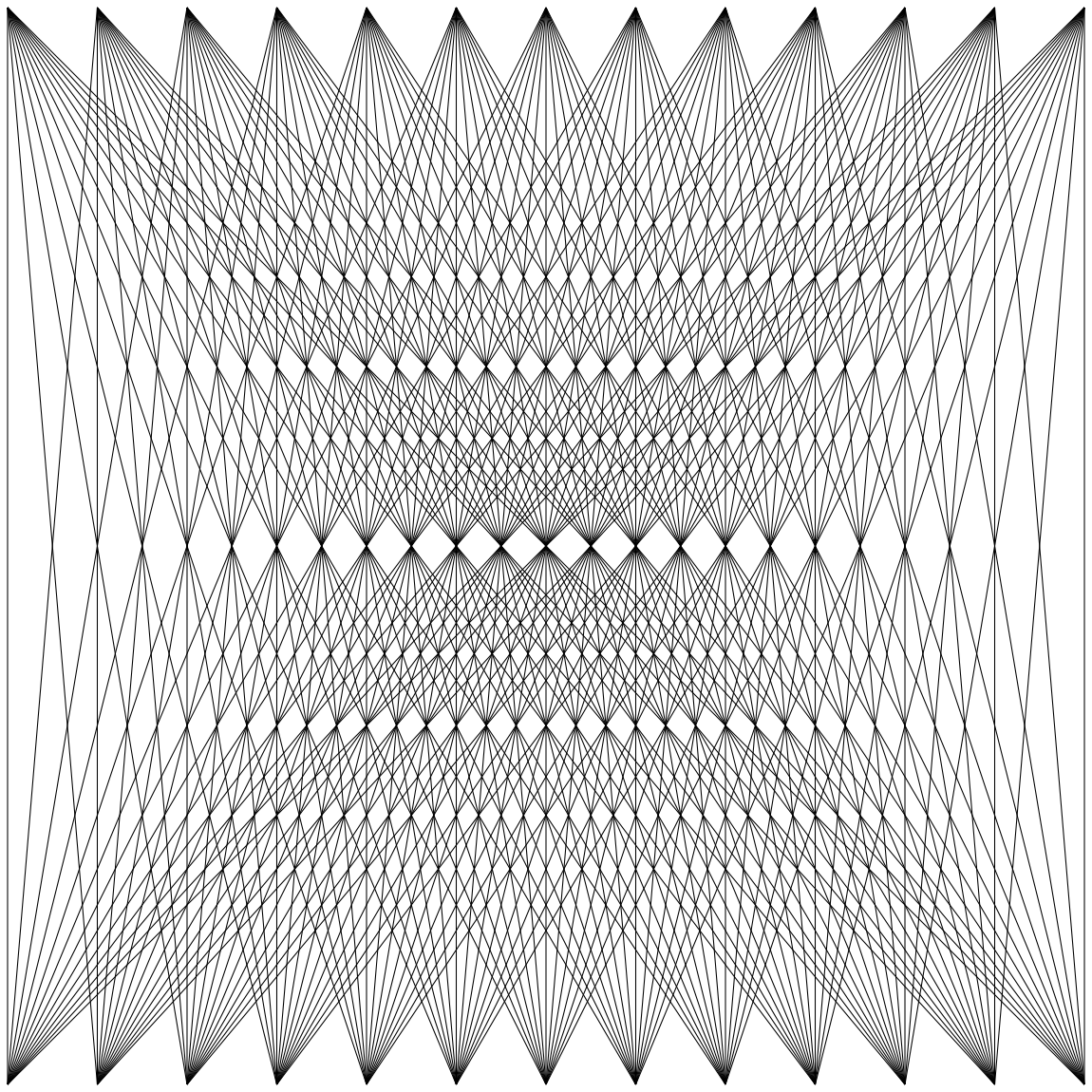


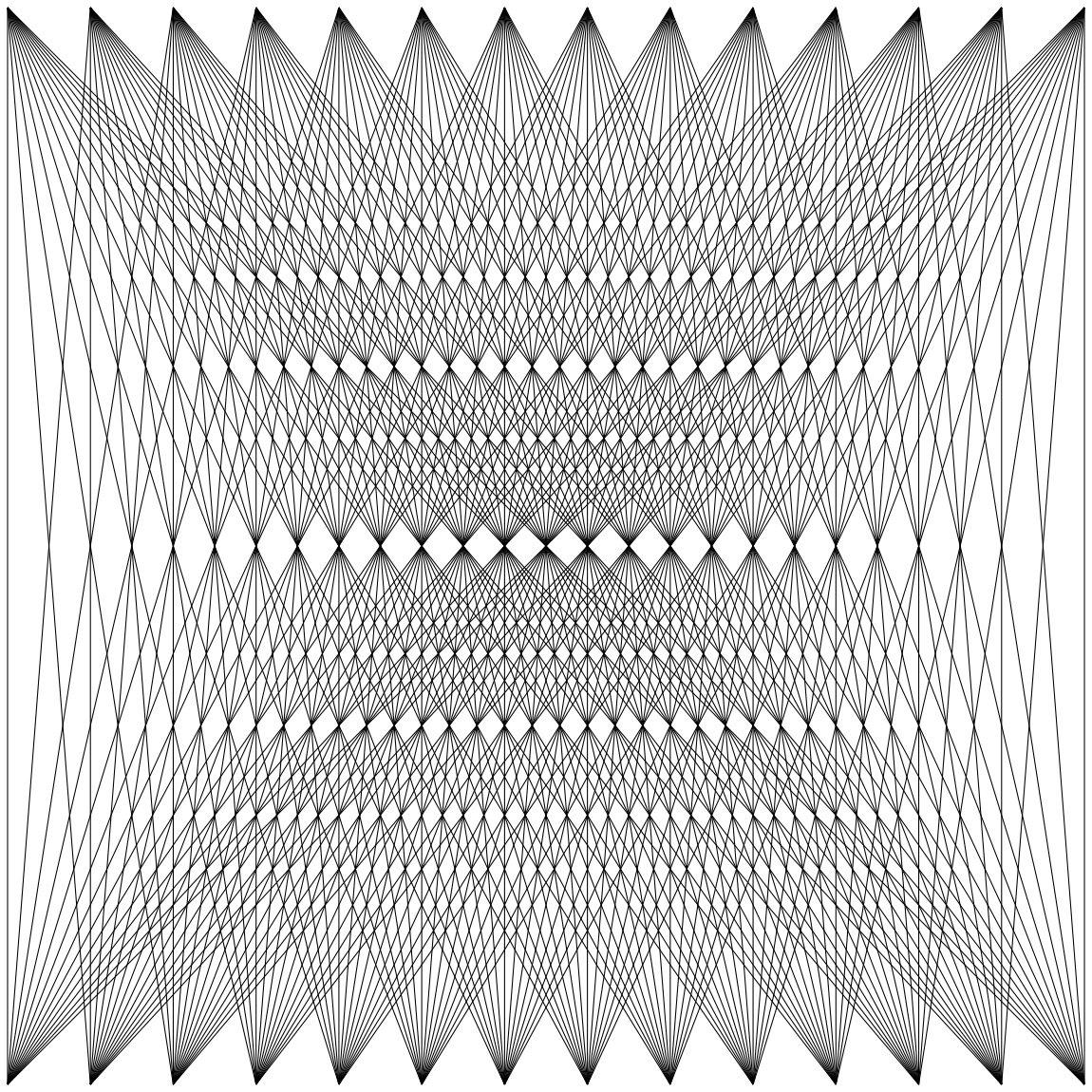


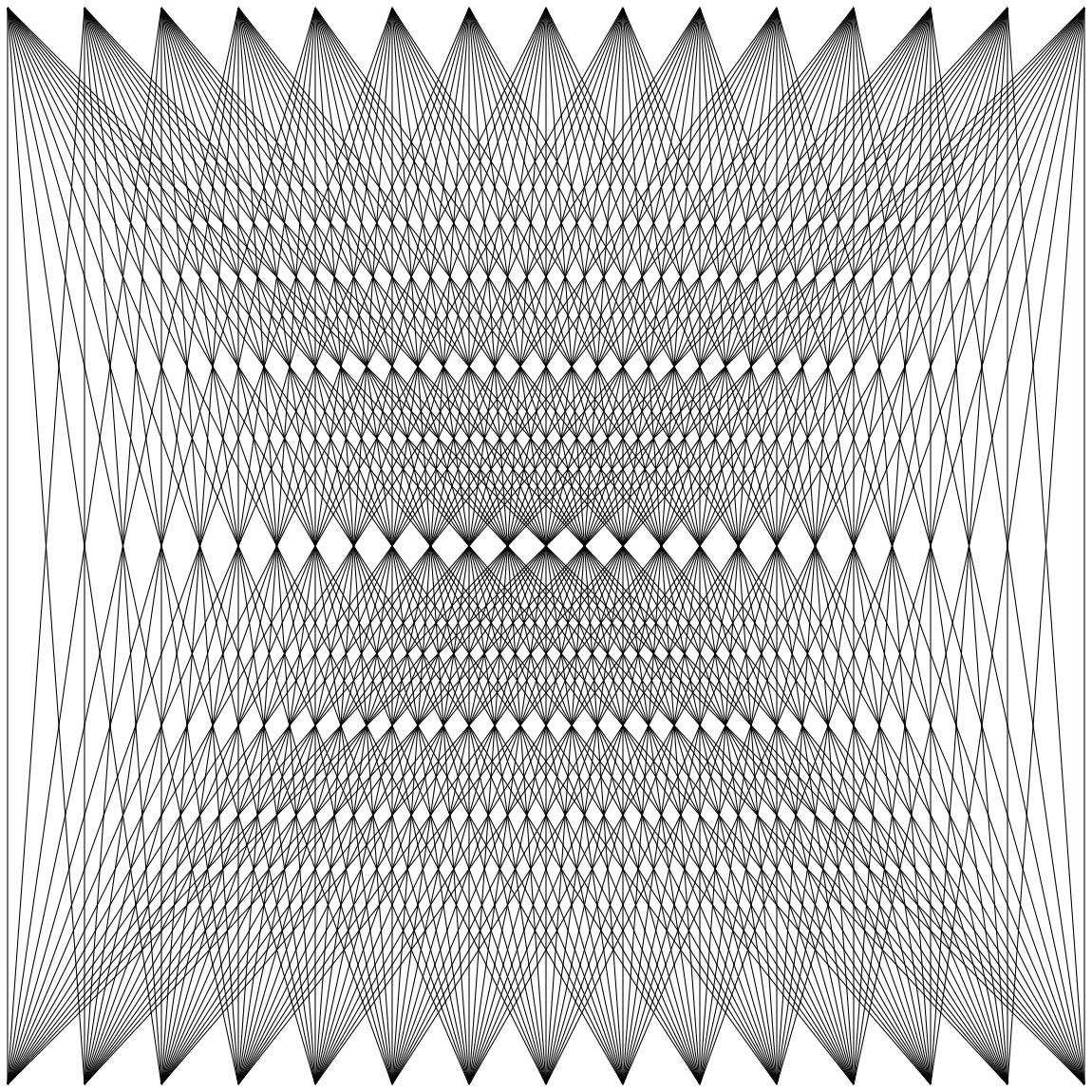


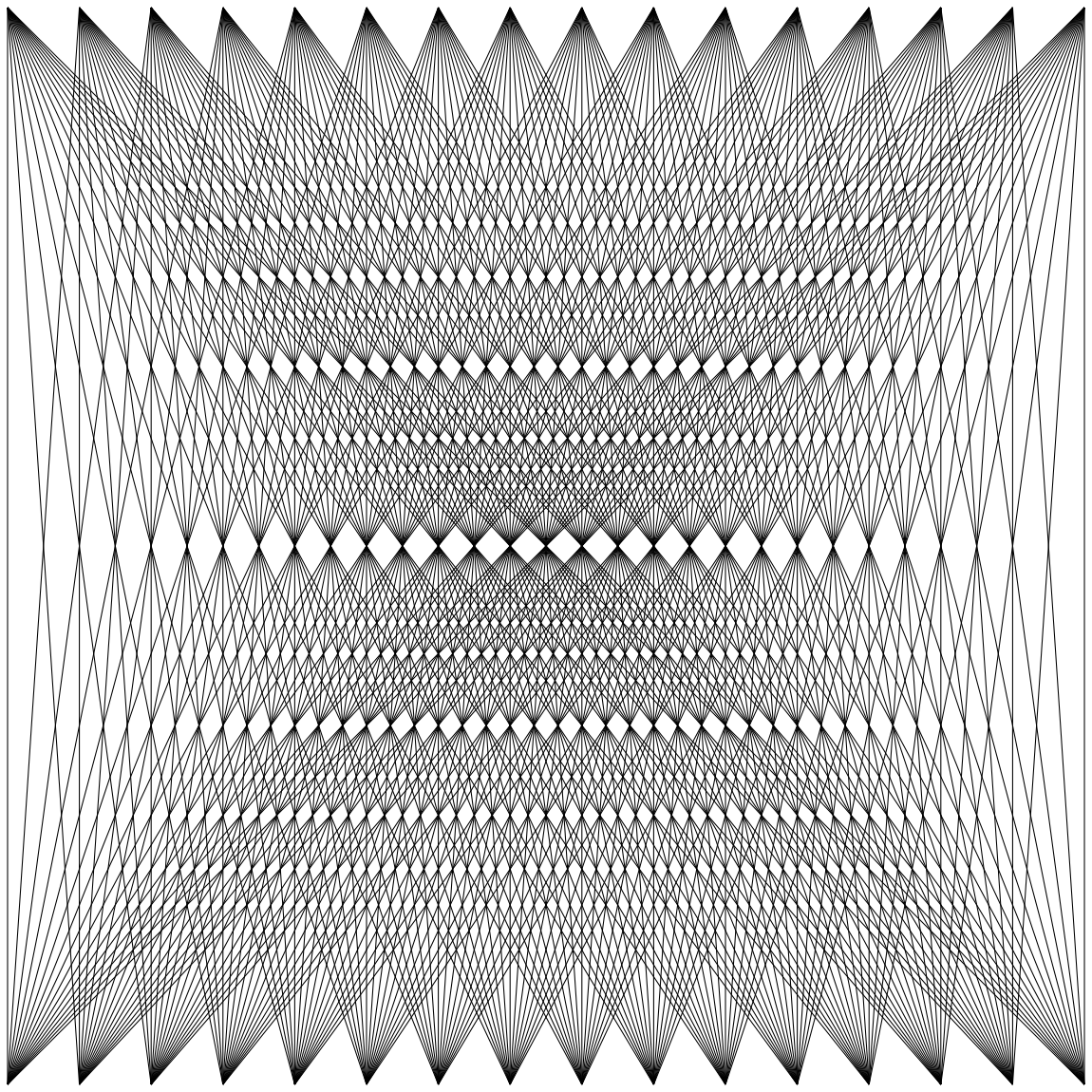


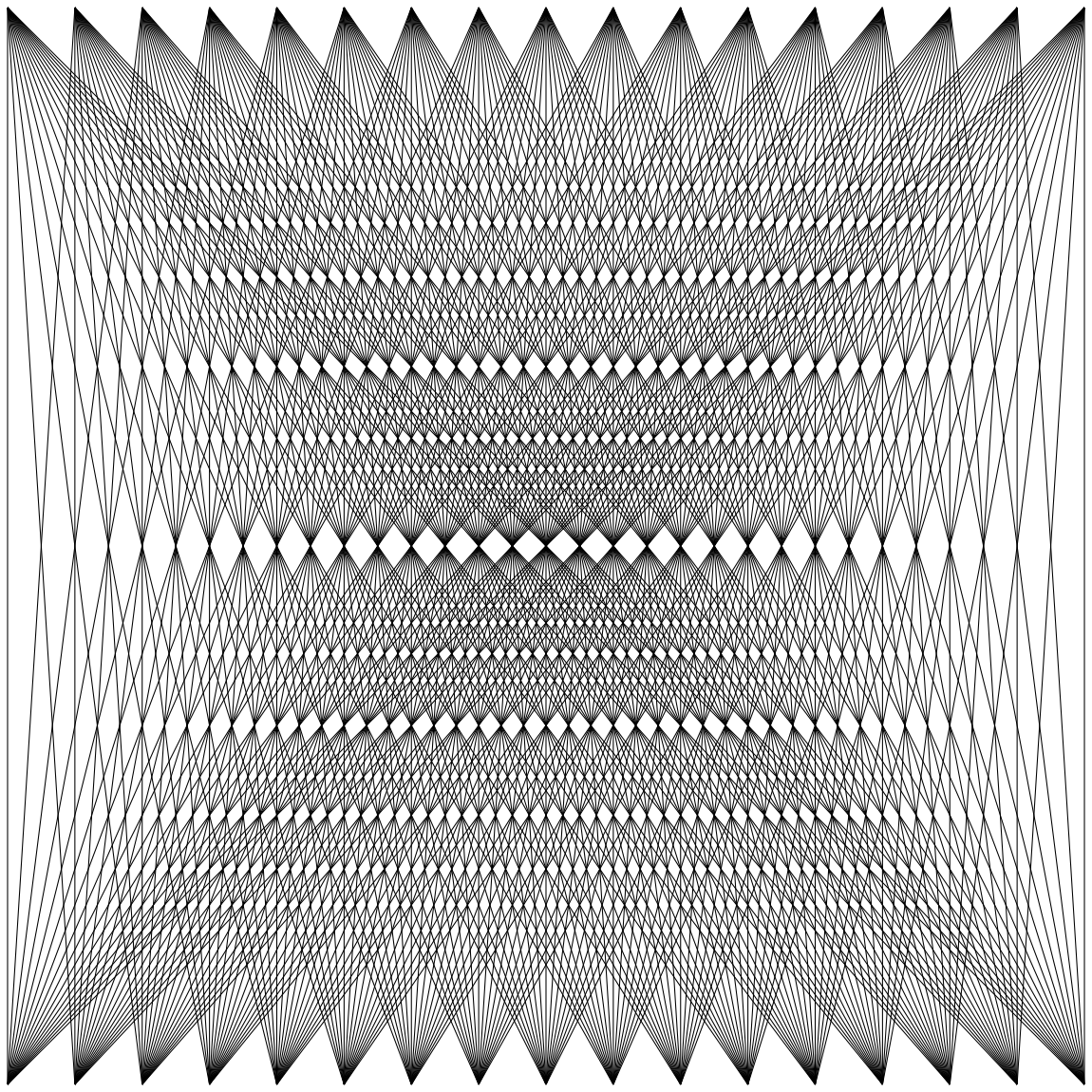


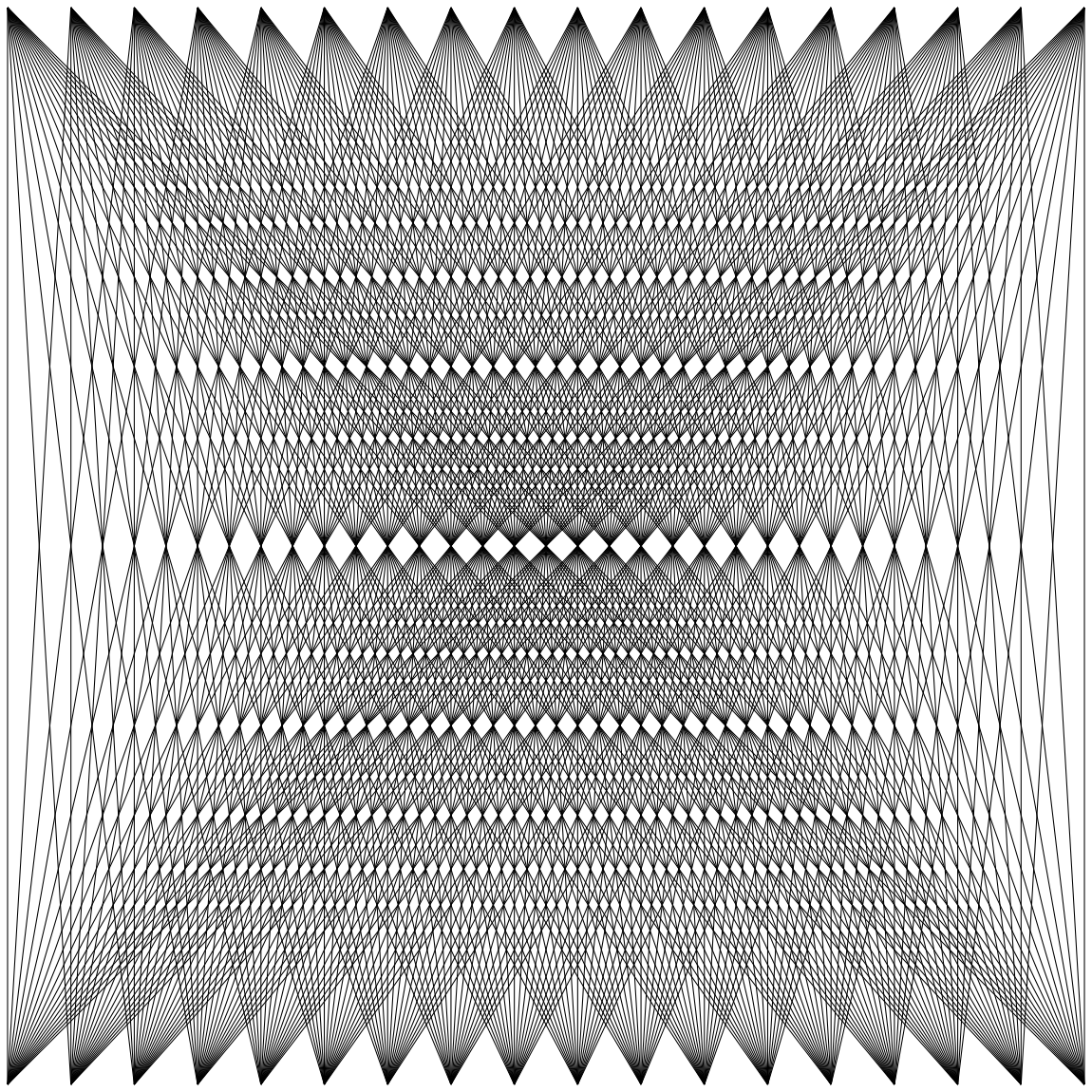


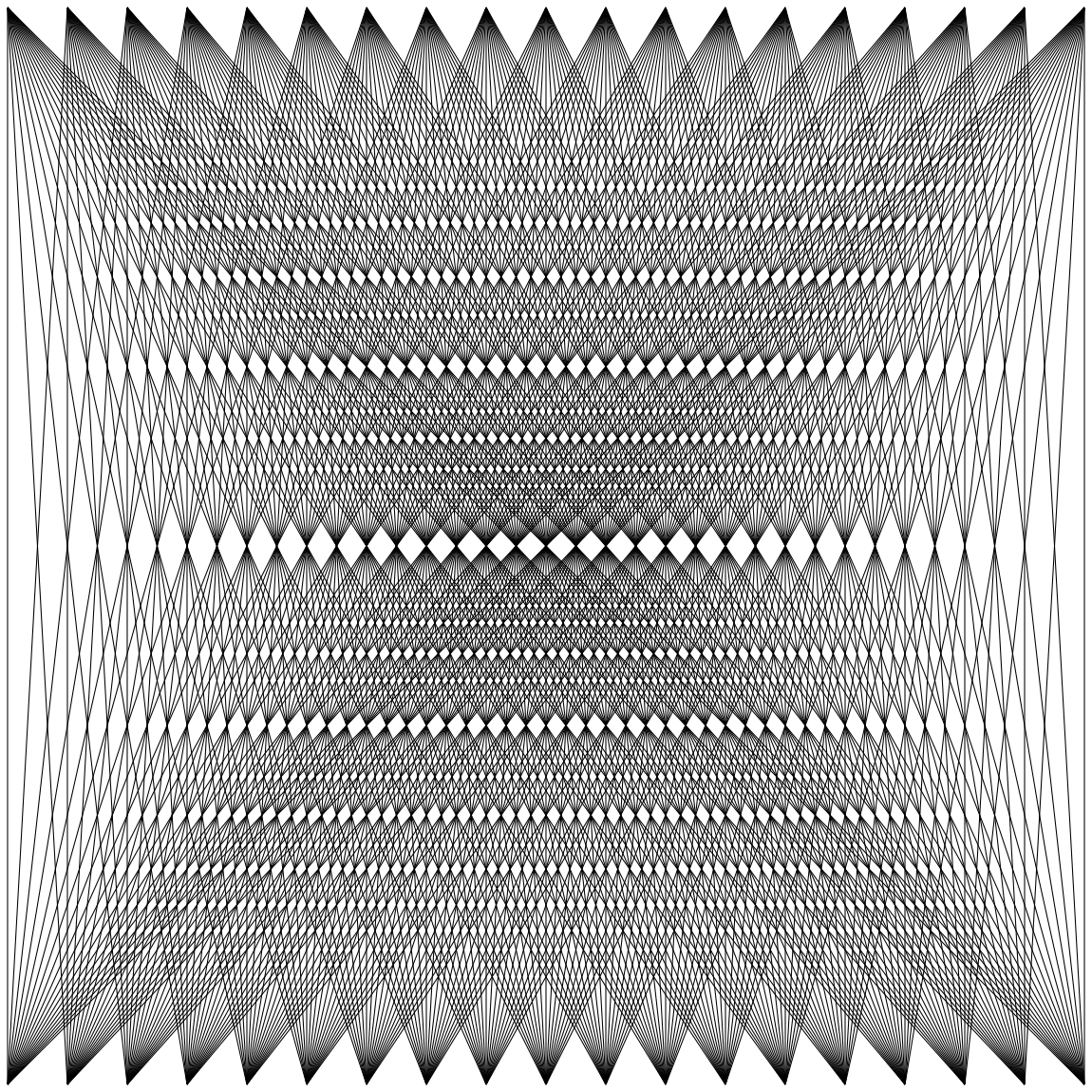


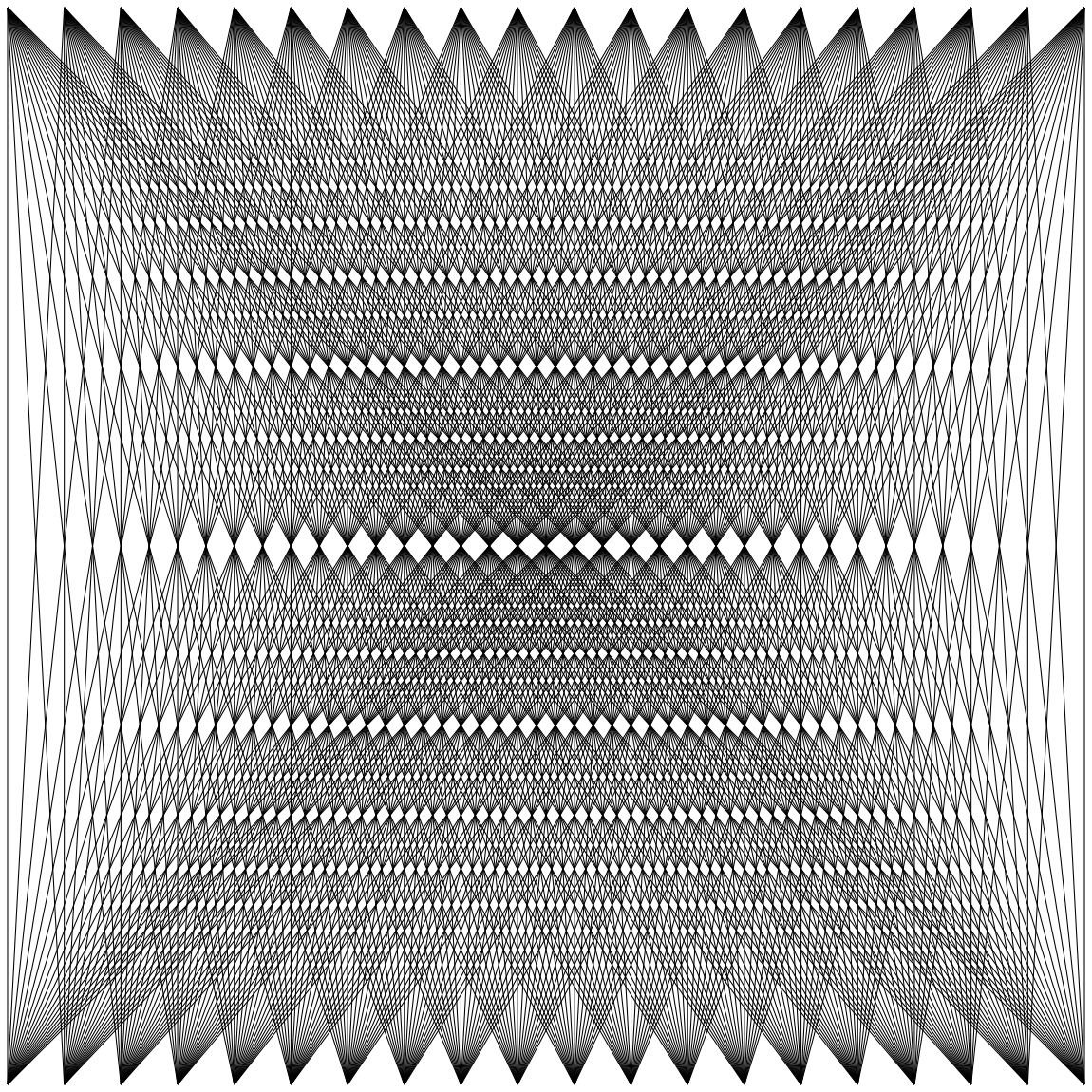


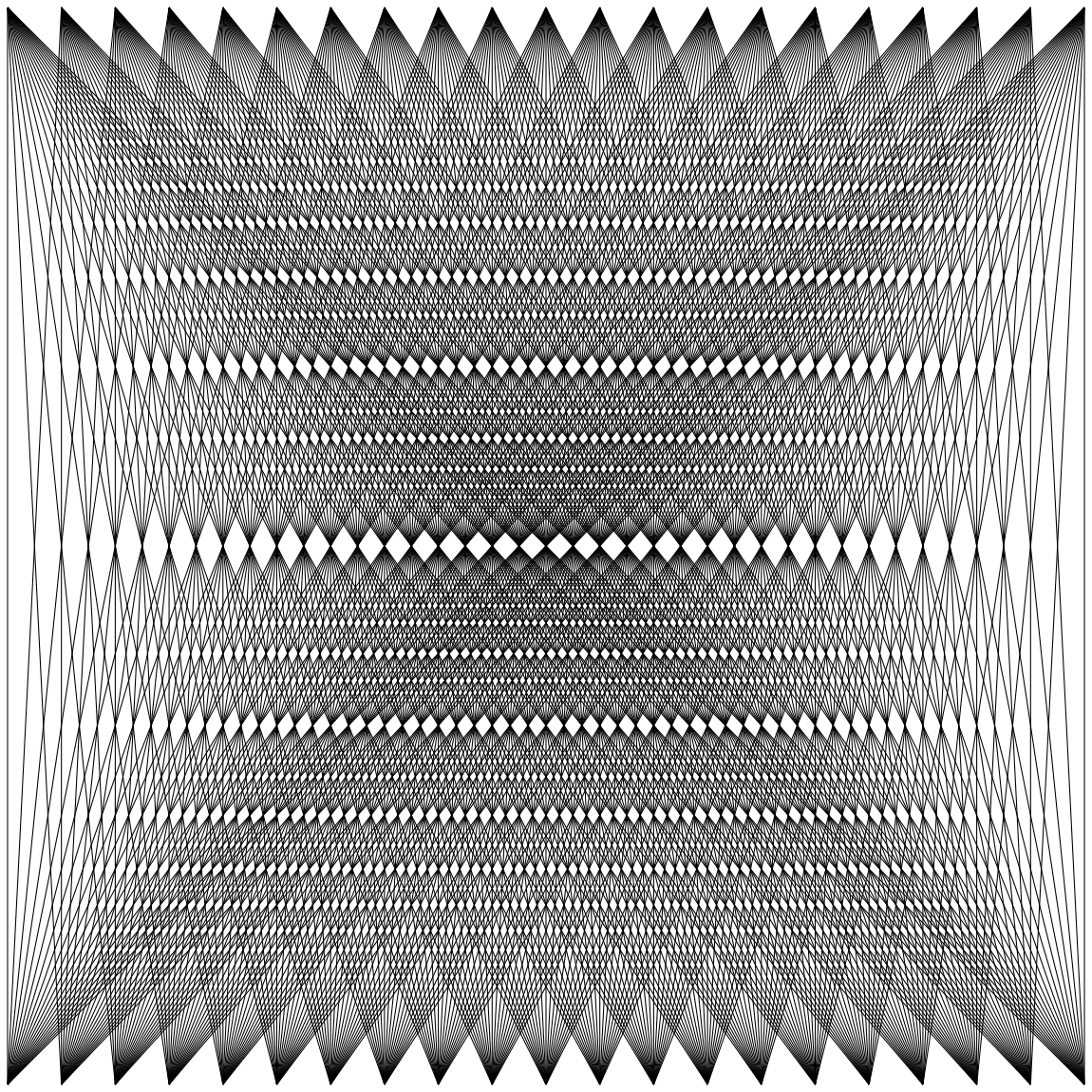






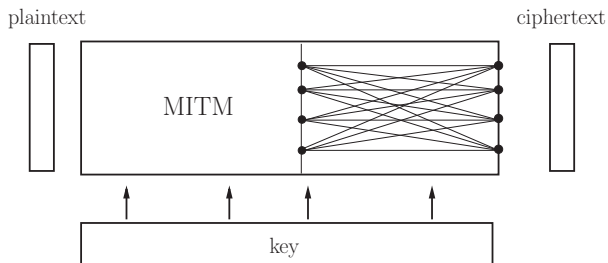






Where?

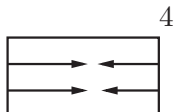
In a cipher



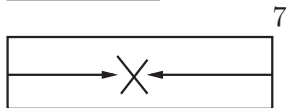
What for?

AES-128

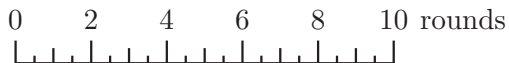
Best meet-in-the-middle
attack on AES-128



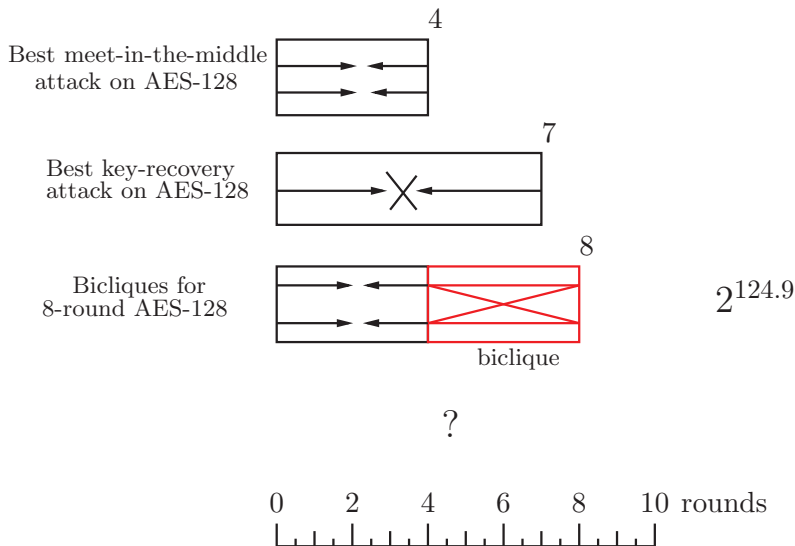
Best key-recovery
attack on AES-128



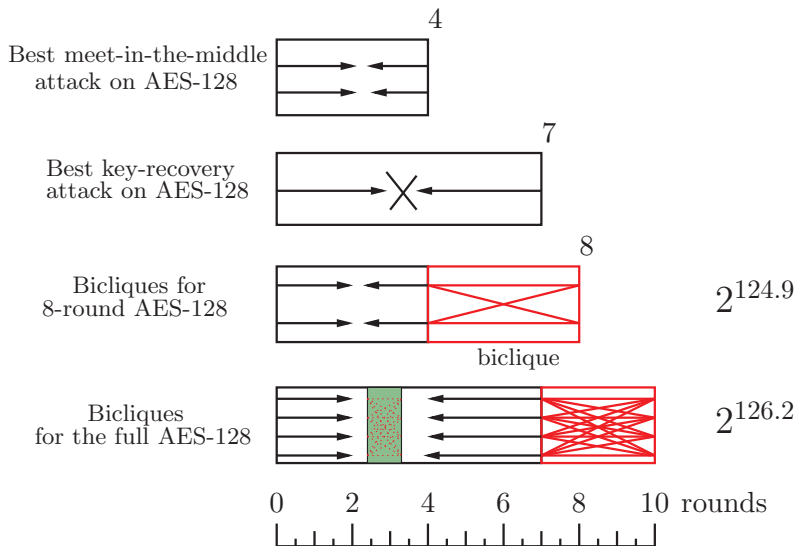
?



AES-128

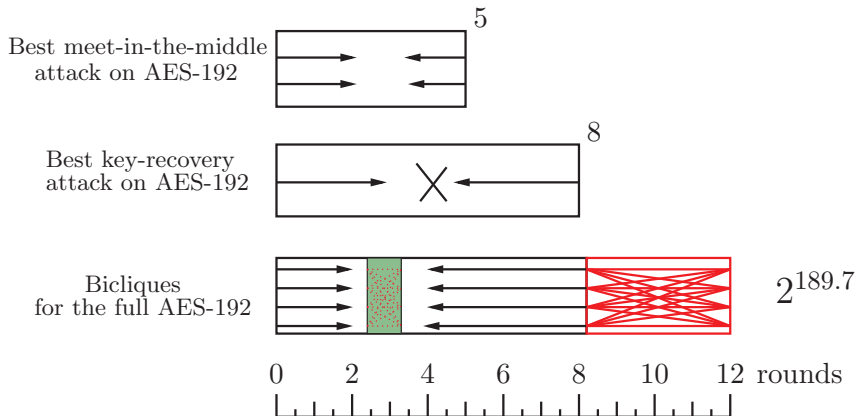


AES-128



192?

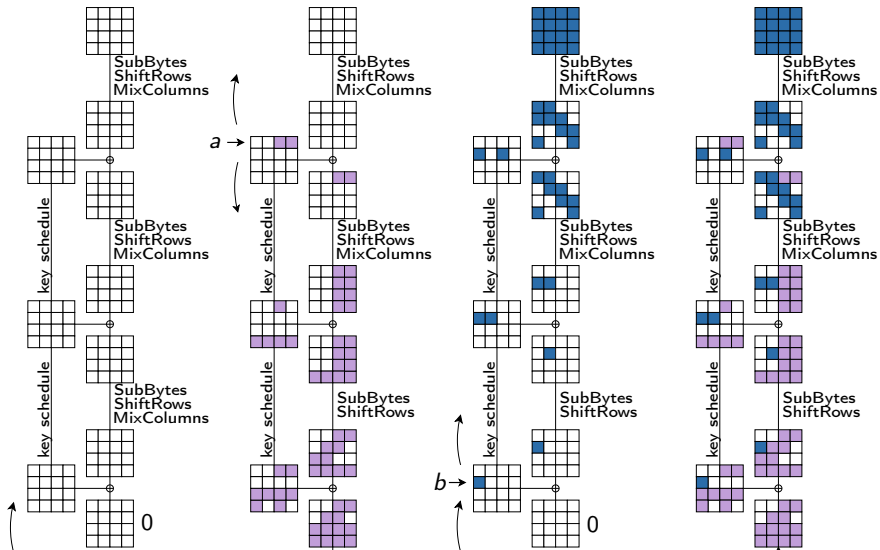
Sure

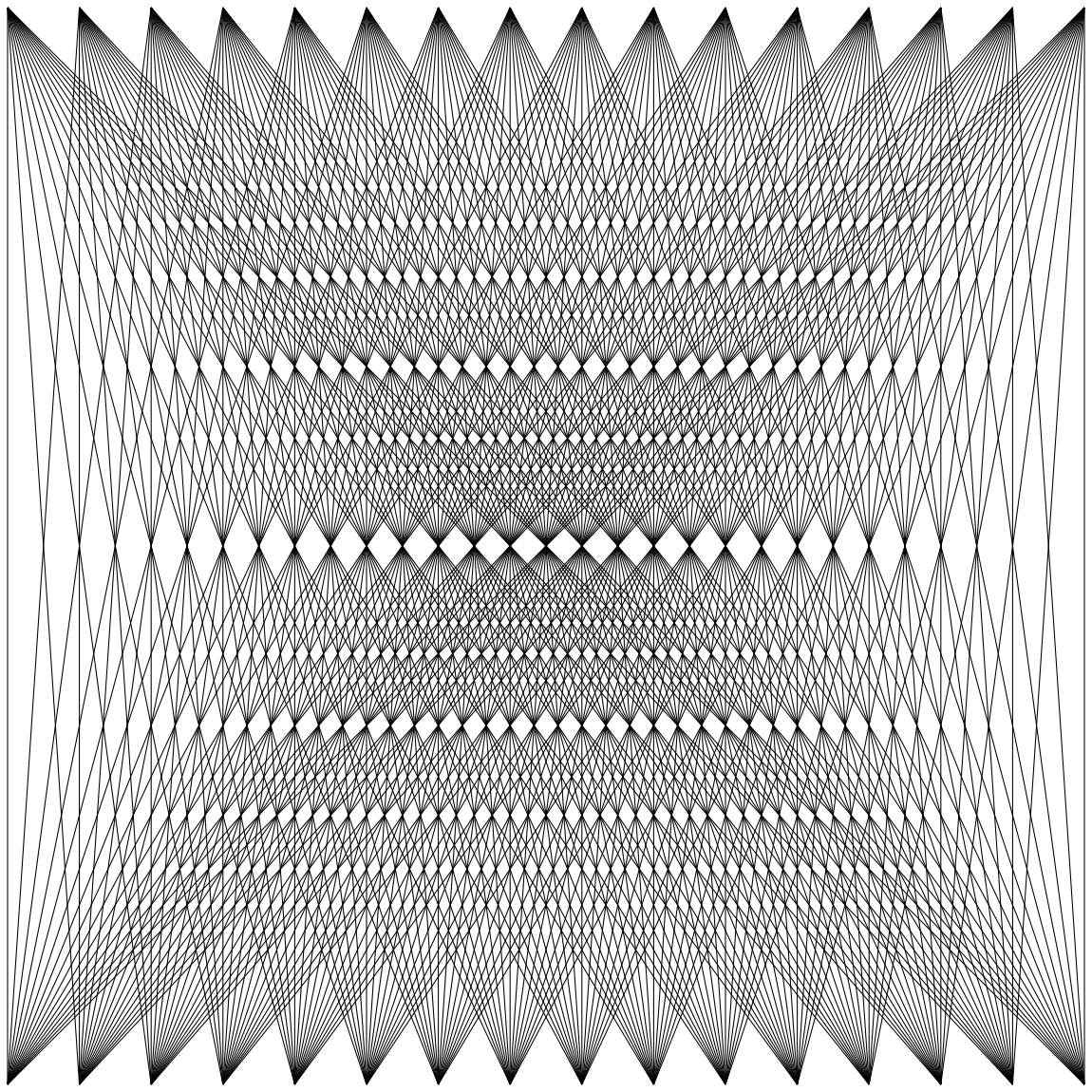


Methods?

AES-128

3-Round Biclique of Higher Dimension





- Split the 2^{128} key space into groups of 2^{16} keys
- To test all 2^{16} keys in a group:
 - Perform a base computation
 - Precompute 2^8 forward key modifications
 - Precompute 2^8 backward key modifications
 - For each key in 2^{16} , combine one forward and one backward computation for free
- ALL 2^{16} keys in the group covered with only 2^9 computations!

Biclique Key Recovery for AES

rounds	computations	data	memory	success prob.
AES-128 secret key recovery				
10 (full)	$2^{126.18}$	2^{88}	2^8	1
AES-192 secret key recovery				
12 (full)	$2^{189.74}$	2^{80}	2^8	1
AES-256 secret key recovery				
14 (full)	$2^{254.42}$	2^{40}	2^8	1

No related keys!

Check the full paper at the project website

<http://research.microsoft.com/en-us/projects/cryptanalysis/aes.aspx>