Onions and Keys

asn

Euclid

- Elements
- Infinity of primes
- Perfect numbers

Euclid's Greatest Common Divisor algorithm (GCD)

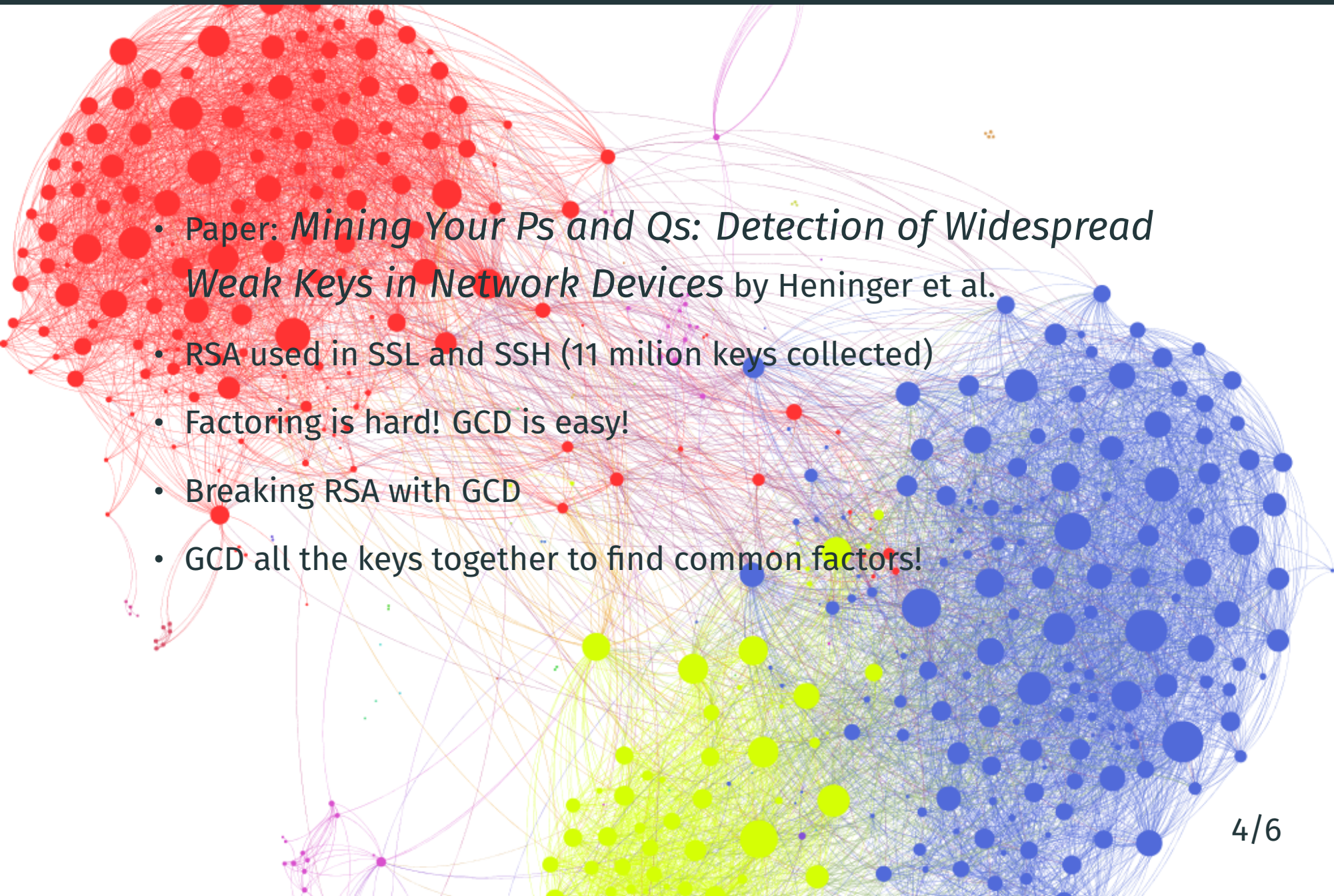
Algorithm 1 Euclid's algorithm

```
1: procedure EUCLID(a, b)                    ▷ The g.c.d. of a and b
2:     r ← a mod b
3:     while r ≠ 0 do                        ▷ We have the answer if r is 0
4:         a ← b
5:         b ← r
6:         r ← a mod b
7:     end while
8:     return b                              ▷ The gcd is b
9: end procedure
```

Greatest Common Divisors examples

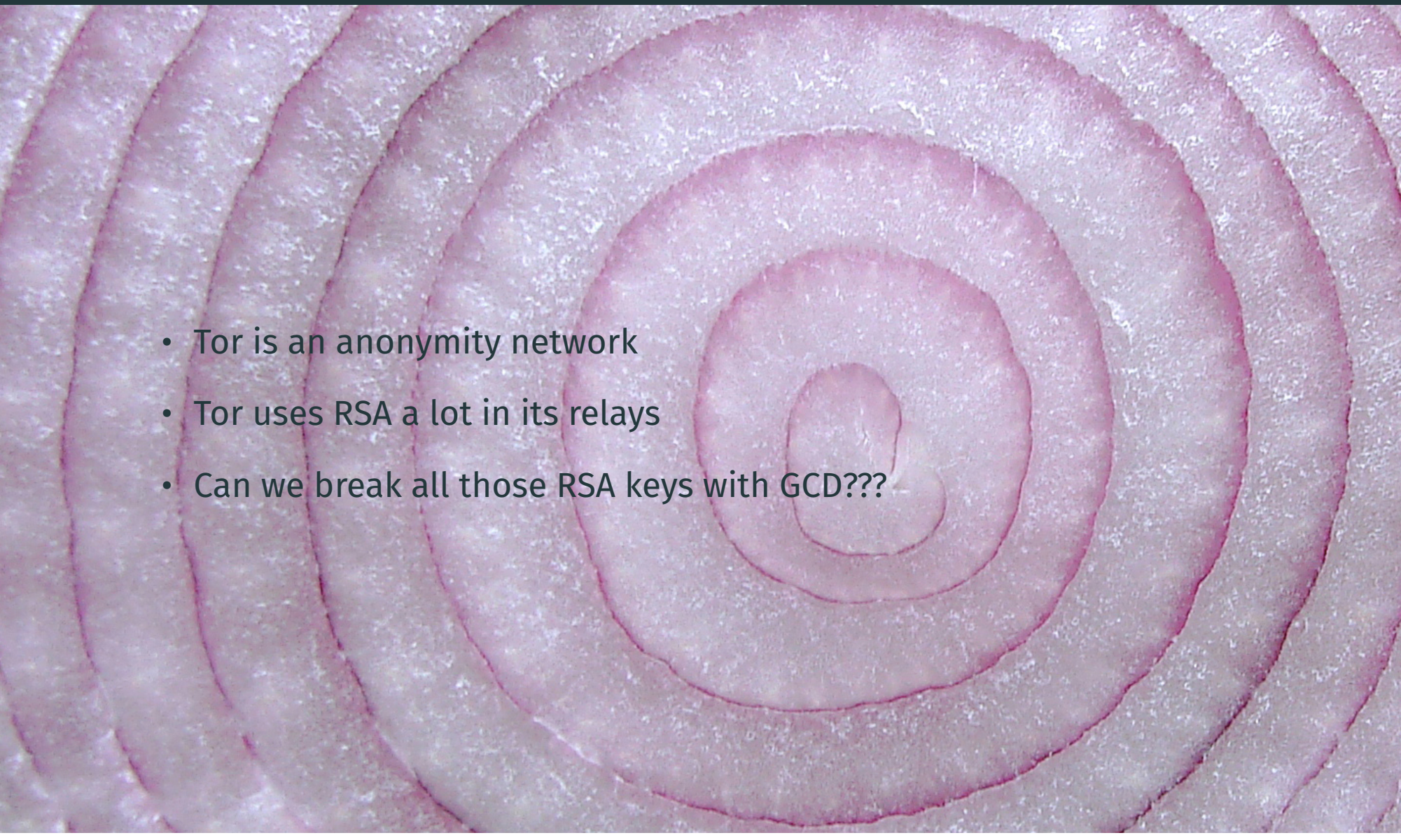
- gcd(4, 10) = 2
- gcd(6, 15) = 3
- gcd(12, 60) = 12
- gcd(3, 5) = 1

Breaking The Internet With GCD



- Paper: *Mining Your Ps and Qs: Detection of Widespread Weak Keys in Network Devices* by Heninger et al.
- RSA used in SSL and SSH (11 milion keys collected)
- Factoring is hard! GCD is easy!
- Breaking RSA with GCD
- GCD all the keys together to find common factors!

A Look Into Tor Keys



- Tor is an anonymity network
- Tor uses RSA a lot in its relays
- Can we break all those RSA keys with GCD???

Thanks!