



**TECHNISCHE  
UNIVERSITÄT  
DRESDEN**

**Department of Computer Science** Institute of System Architecture, Operating Systems Group

# **THE MATHEMATICS OF OBSCURITY**

**HERMANN HÄRTIG,  
CLAUDE-JOACHIM HAMANN,  
MICHAEL ROITZSCH**

I will tell about...

- the process of finding **security errors**
- our **mathematical model** for it
- the **comparison** of open and closed source

I will not tell about...

- whether open or closed source is **better**

## Open Source

everyone has access  
to source code

everyone can search  
for bugs

more defenders find  
more bugs

easier to find bugs

## Closed Source

only the company has  
the source code

attackers have a  
harder time

bugs are prevented  
from being exploited

harder to find bugs

**Attackers only need only one error.  
Defenders need to find all errors.**



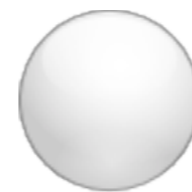


**3 Errors:**



$$e = 3$$

**No Error:**

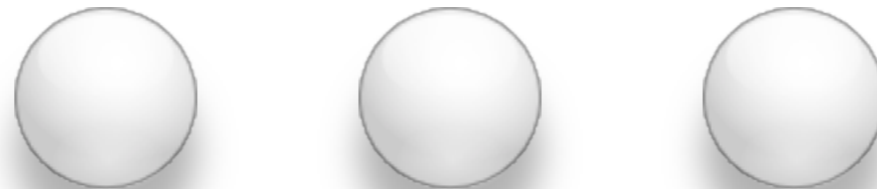


$$p, q$$

# ATTACKERS



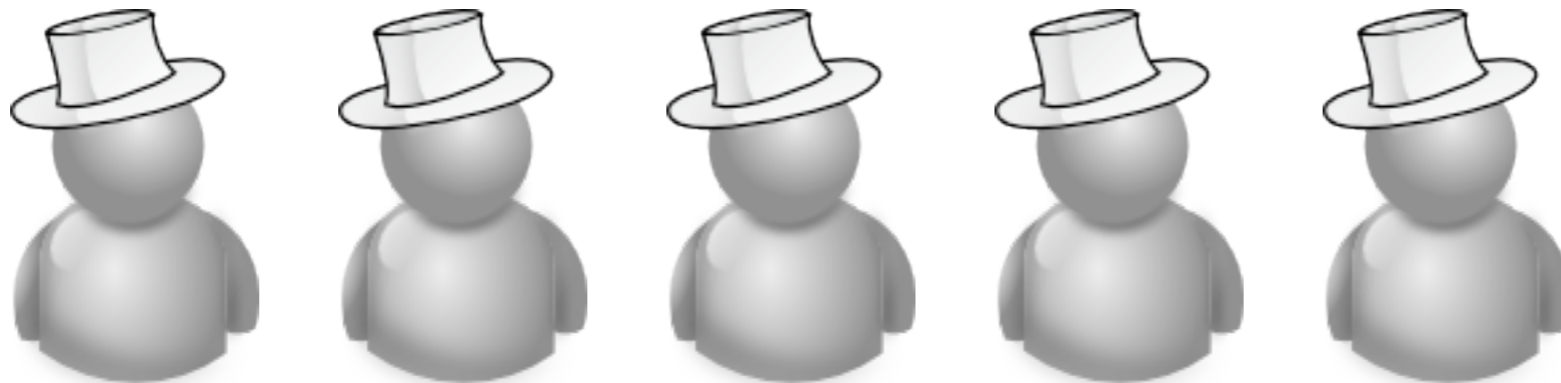
$$a = 3$$





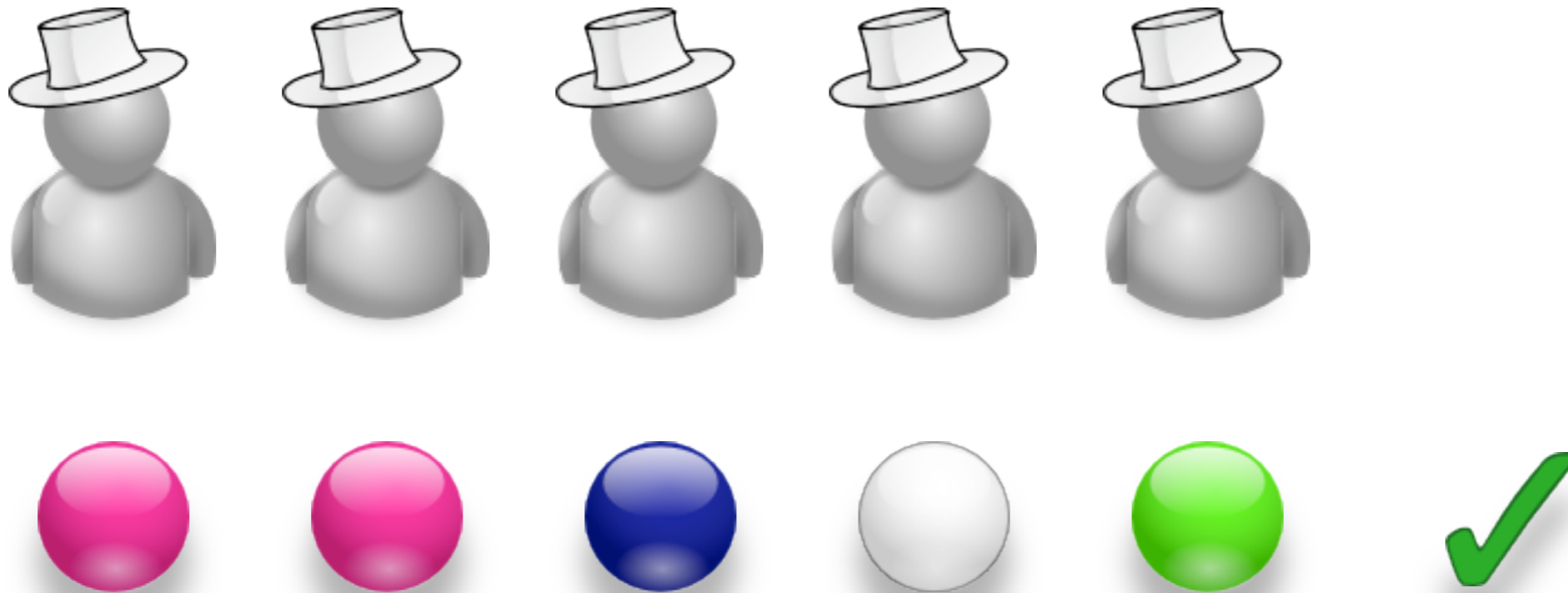
$$p_A = 1 - (1 - ep)^a$$





$$d = 5$$





$$p_D = e! \cdot \sum_{i=0}^{d-e} \binom{d}{i} q^{d-i} (1 - eq)^i S_{d-i,e}$$

- 20 errors

$$e = 20$$

- 1% probability to find an error

$$p = q = 0.01$$

- 75% desired winning chance

$$p_A = p_D = 0.75$$

- How many attackers?

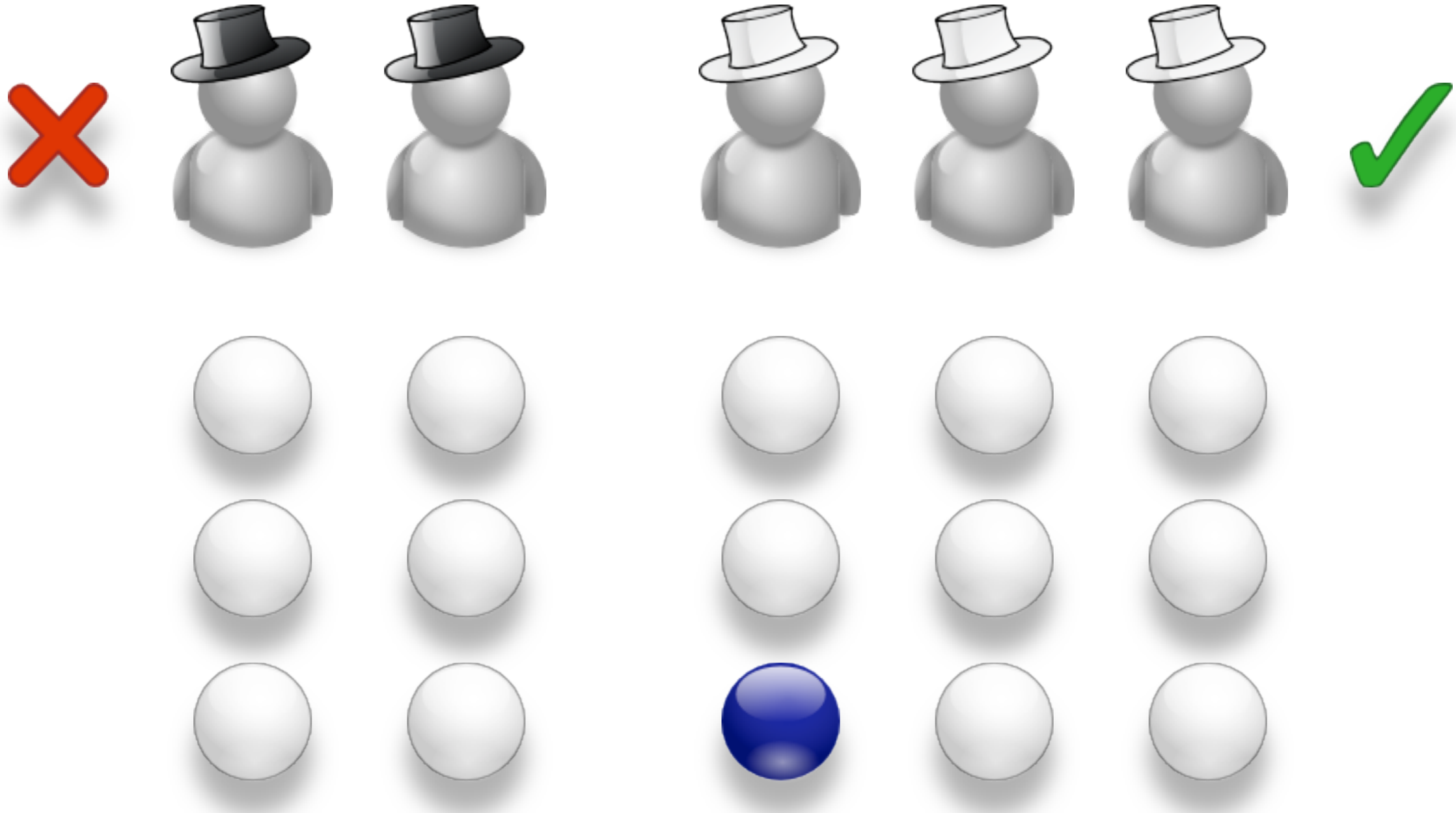
$$a = 7$$

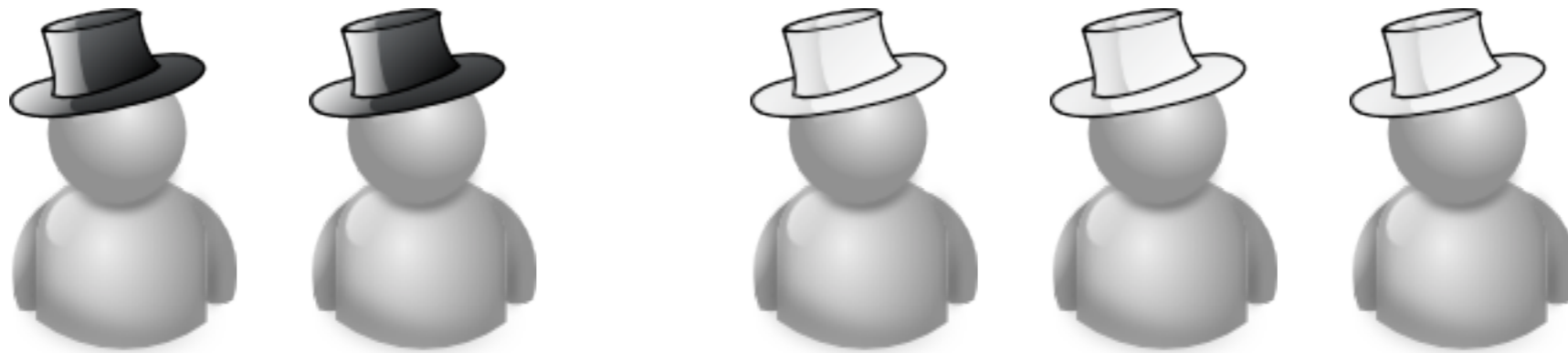
- How many defenders?

$$d = 424$$

- What happens if both sides lose?
- ... or win?
- Do the defenders really lose if they do not find all errors?
- They just have to find the errors **first**.
- Instead of a snapshot, model a **race**.

**Defenders need to find any error  
earlier than the attackers.**





$p$

$m$  steps

$q$

$n$  steps

$$p_{m,n} = \underbrace{(1 - p)^{m-1} p}_{\text{black hat}} \cdot \underbrace{(1 - q)^{n-1} q}_{\text{white hat}}$$

$$p_{m,n} = (1 - p)^{m-1} p \cdot (1 - q)^{n-1} q$$

defenders win for  $n < m$

$$p_W = \sum_{n=1}^{\infty} \sum_{m=n+1}^{\infty} p_{m,n} = \frac{q(1-p)}{q(1-p) + p}$$



$$p_W = \sum_{n=1}^{\infty} \sum_{m=n+1}^{\infty} p_{m,n} = \frac{q(1-p)}{q(1-p) + p}$$

**open  
source**

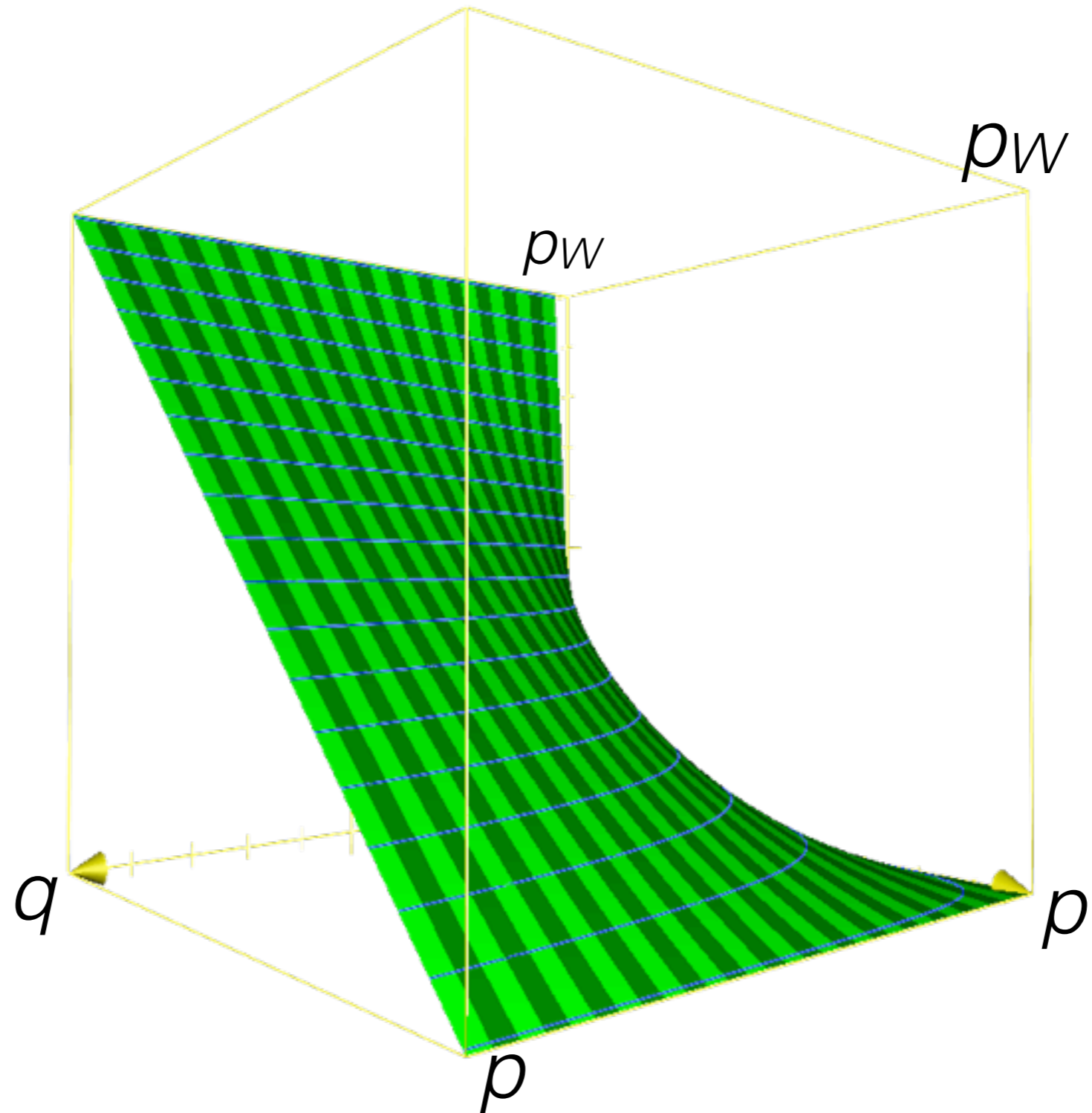
**more  
defenders**

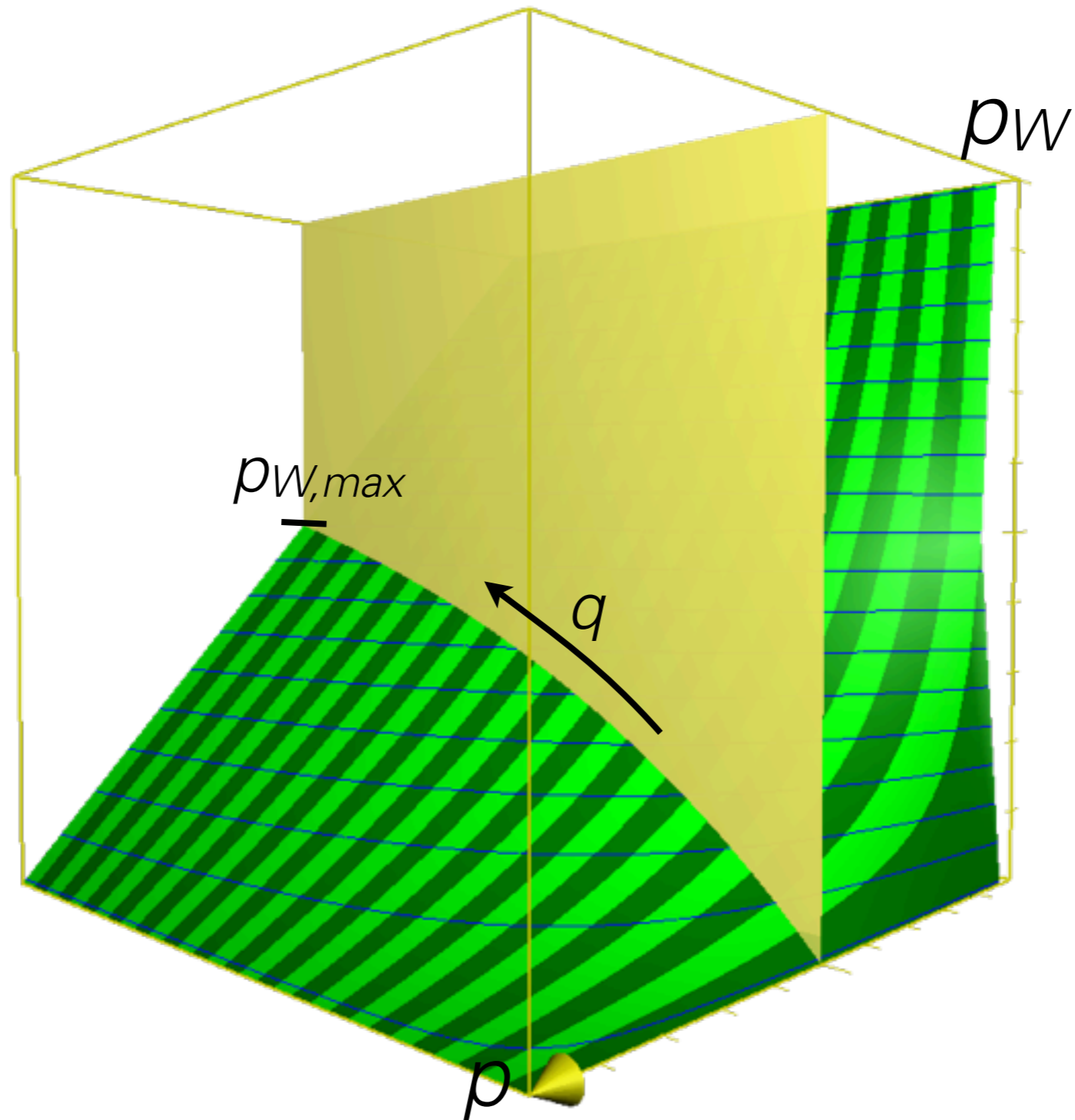
**higher q**

**closed  
source**

**harder for  
attackers**

**lower p**





- 1 million lines of code, 15 security errors  
 $e = 15$
- probability for a single defender to find an error  
 $q_{single} = 0.002\%$
- the same for attackers in open source case  
 $p_{single,open} = 0.002\%$
- closed source factor 2 harder  
 $p_{single,closed} = 0.001\%$
- 500 attackers
- How many defenders do we need?

	<b>pw = 0.6</b>	<b>pw = 0.9</b>
<b>closed source</b>	<b>7815</b>	<b>62088</b>
<b>open source</b>	<b>17133</b>	<b>impossible</b>

**No matter how many defenders,  
there's always a window for attackers.**

- urn model for discovery of security errors
- race between attackers and defenders
- there is an upper bound for the defenders
- this bound may be hit in reality