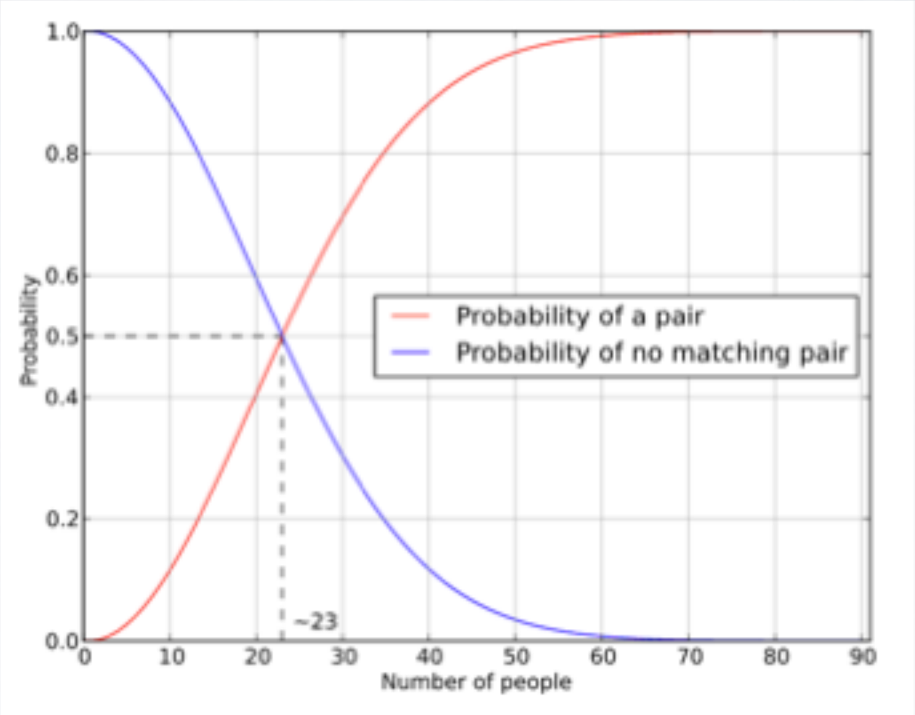
# Birthday Paradox



*"There are 50% chance that 2 people have the same birthday in a room of 23 people"*

**N-bits security**

➡ Given a hash function **H** of **n** bits output, a collision can be found in around $\mathbf{2^{n/2}}$ evaluations

e.g SHA-256 is 128 bits security

# Broken hash functions beyond the birthday paradox

| | Year | Collision |
|---|---|---|
| MD5 | 2013 | $2^{24}$ evaluations ($2^{39}$ with prefix) |
| SHA-1 | 2015 | $2^{57}$ evaluations |