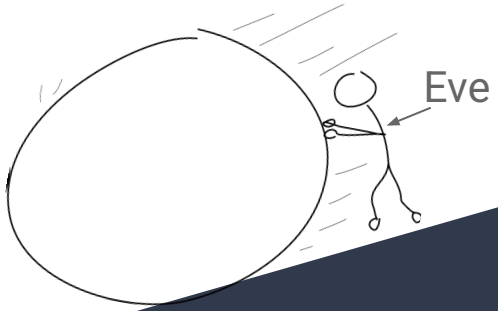
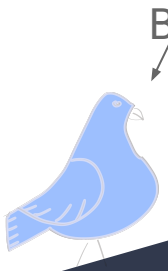
How to explain cost estimation to normal people



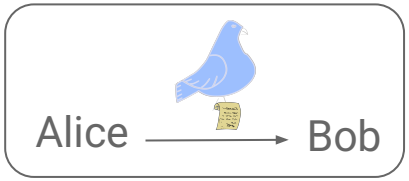


Crypto 2024 Rump Session

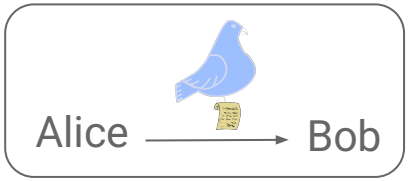
~~KASTEL Science Slam 22.01.24~~

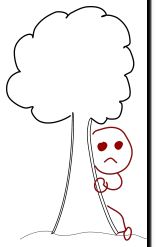
– Marcel Tiepelt

How to do a cost estimation?



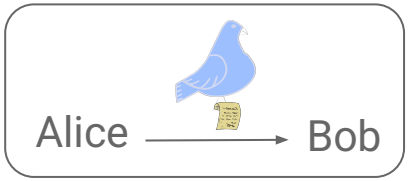
How to do a cost estimation?

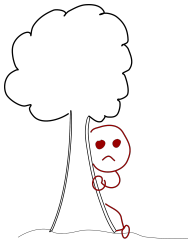




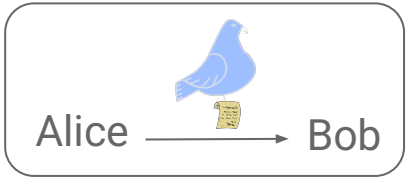
https://xkcd.com/538

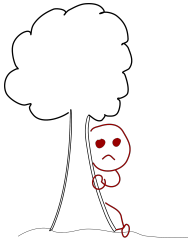
How to do a cost estimation?





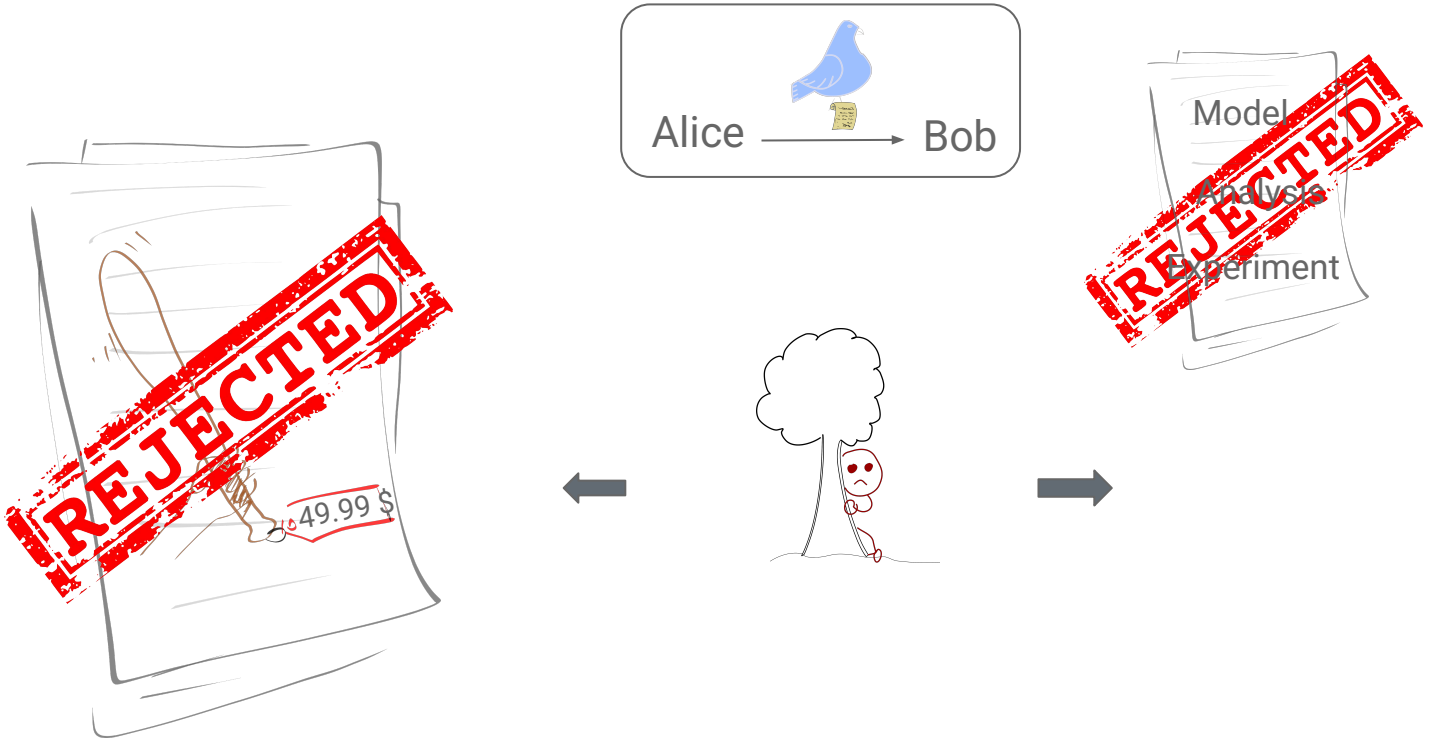
How to do a cost estimation?



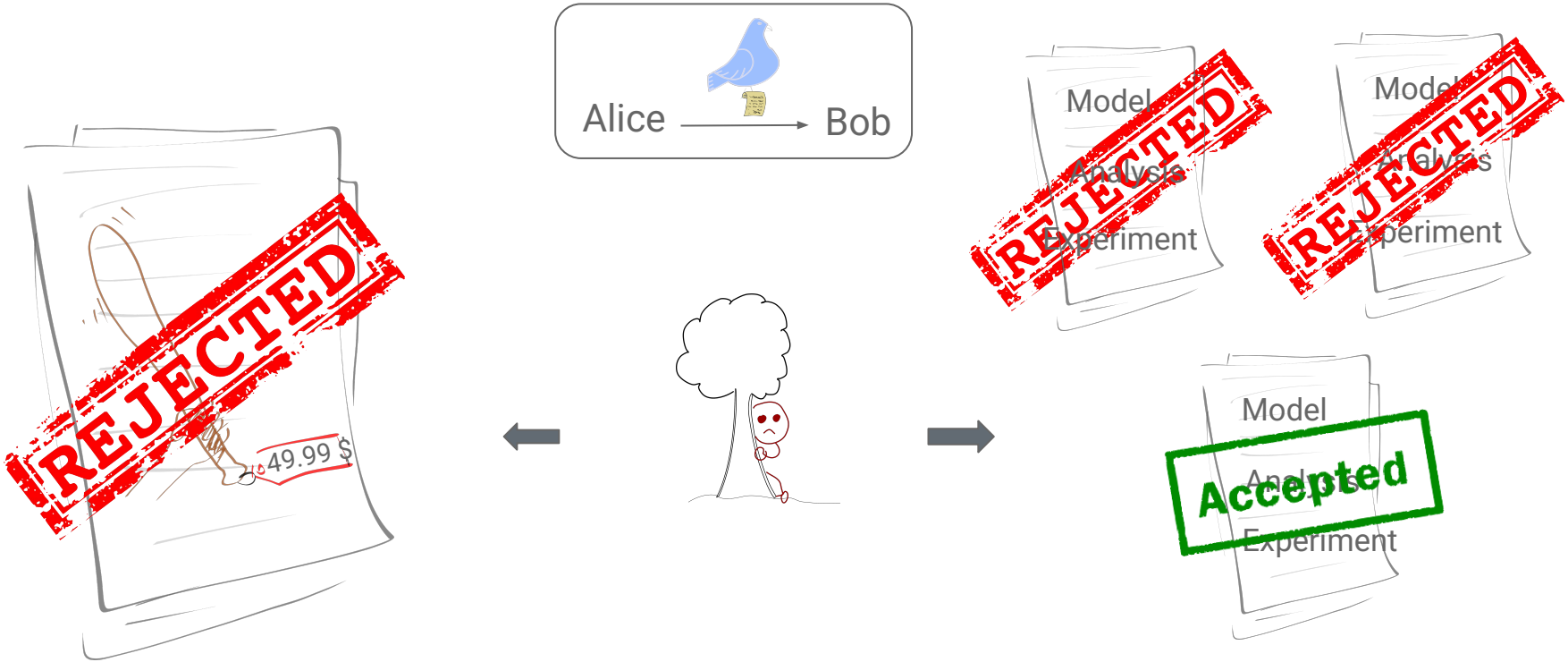


How to do a cost estimation?

How to do a cost estimation?



How to do a cost estimation?



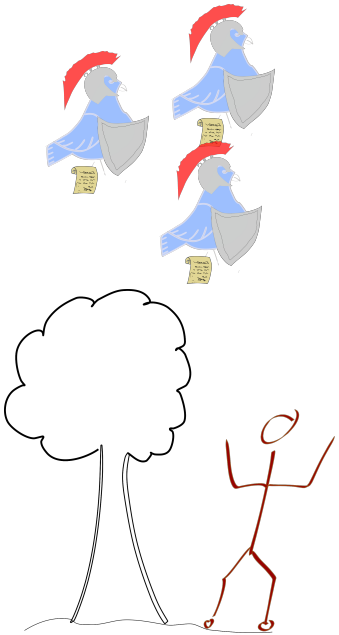
Secure Pigeon Protocol

Secure Pigeon Protocol

Hardness Assumption: Pigeons Indistinguishable

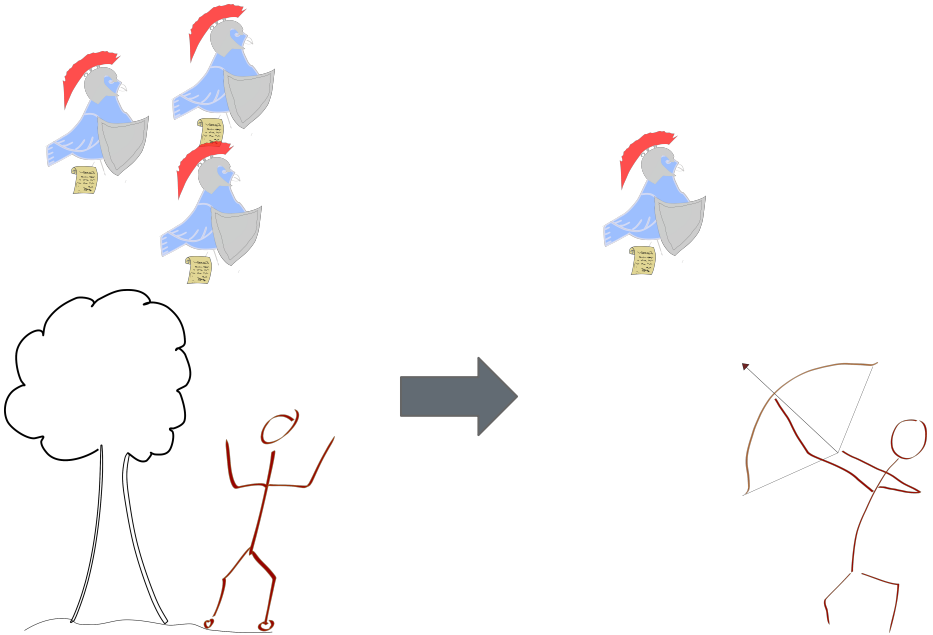
Indistinguishability under Chosen Pigeon Attack (IND-CPA)

Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons…

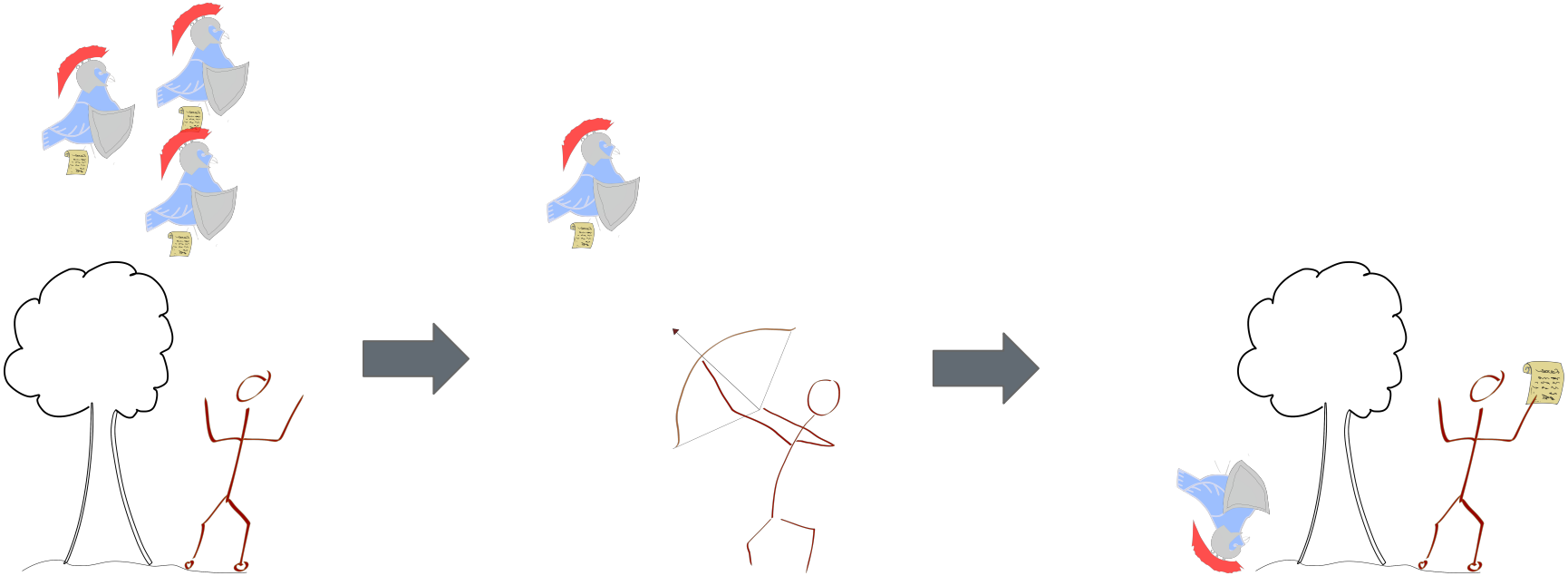
Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons…

… choose one to shoot …

Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons…

… choose one to shoot …

… tell if fake/real message.

Security Proof

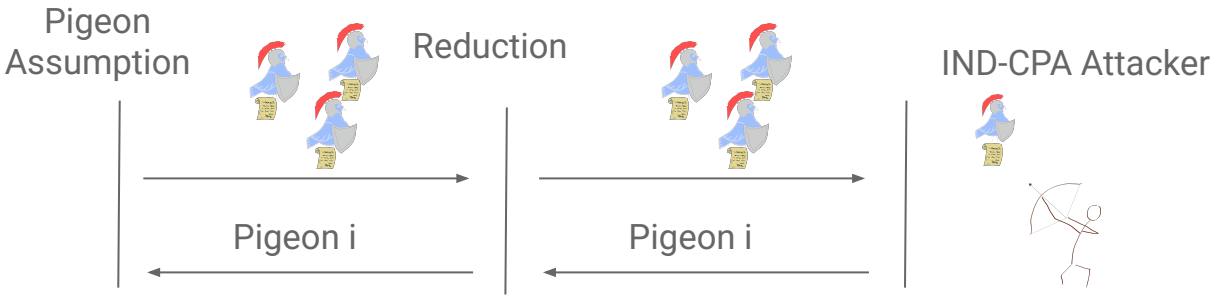
Theorem:
The protocol is IND-CPA secure, unless Eve can distinguish pigeons.

https://xkcd.com/538

Security Proof

Theorem:
The protocol is IND-CPA secure, unless Eve can distinguish pigeons.

Proof:

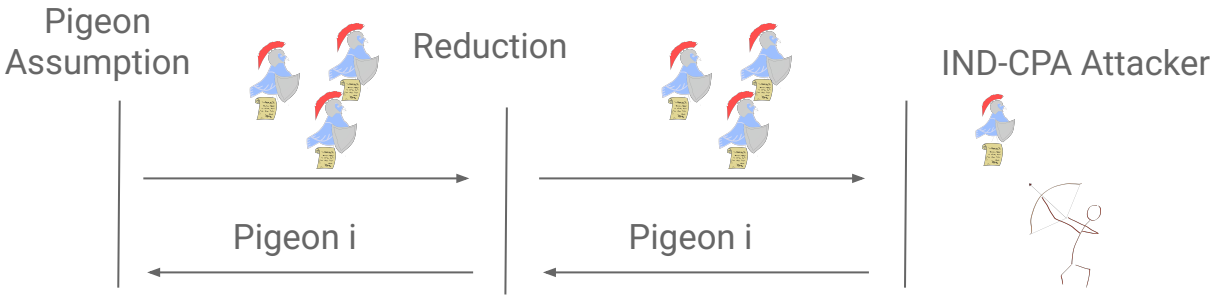


□

Security Proof

Theorem:
The protocol is IND-CPA secure, unless Eve can distinguish pigeons.

Proof:

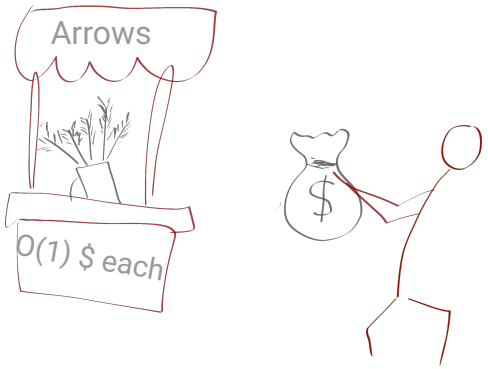


□

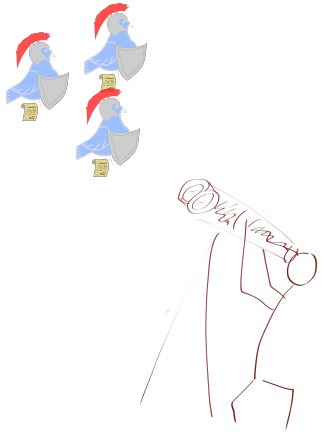
Conclusion:
Pr[Eve learns message] = 1/N
Attack ⇒ Need to shoot **O(N)** Pigeons.

So what is Eve’s cost now?

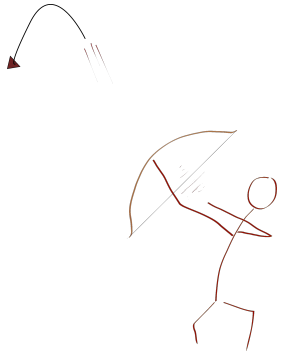
Quantifying Security Costs



How expensive?



Best attack?



Feasibility?

No pigeons were harmed in the making of these slides.