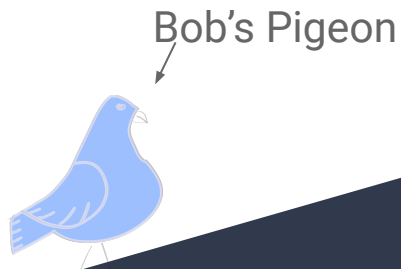


How Big is too Big?

– why quantifying matters to cryptographers.



[...] maximum of 10 minutes [...] present your research in an easily understandable and entertaining way.

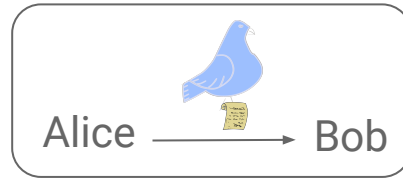
Costing Adversaries against Quantum-secure Cryptography

[...] maximum of 10 minutes [...] present **your research** in an easily understandable and entertaining way.

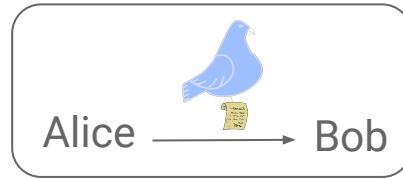
Costing Adversaries ~~against~~ ~~Quantum-secure Cryptography~~

[...] maximum of **10 minutes** [...] present **your research** in an **easily understandable** and **entertaining** way.

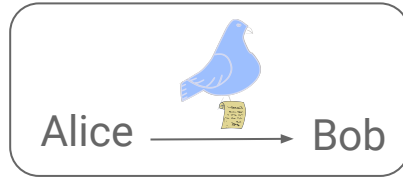
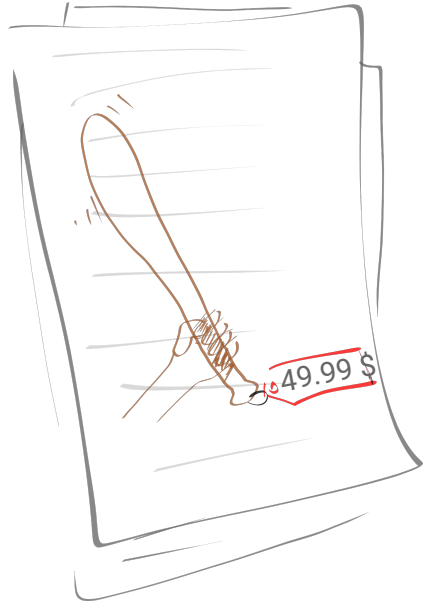
How to do a Cost Analysis?



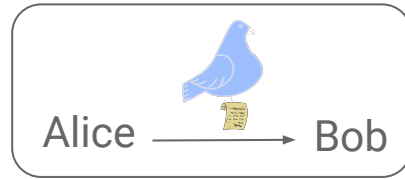
How to do a Cost Analysis?



How to do a Cost Analysis?



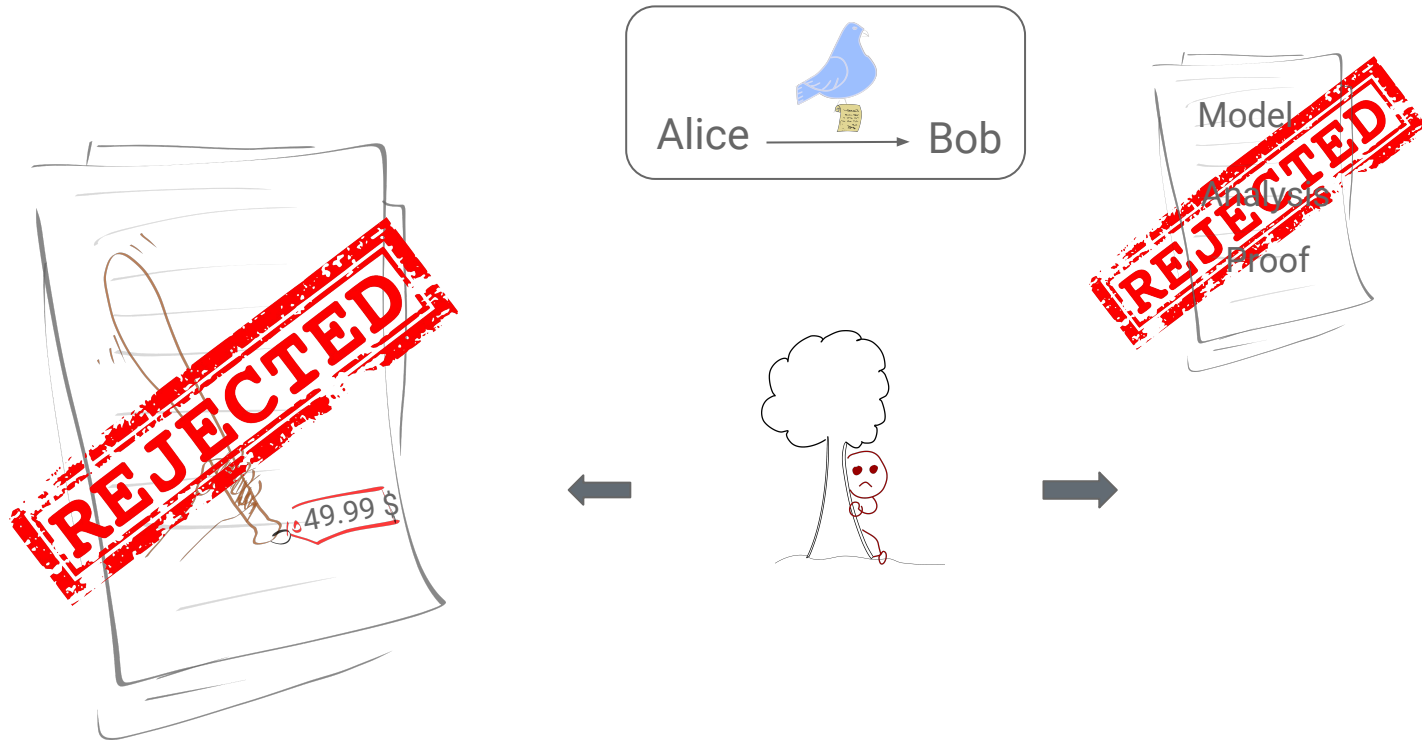
How to do a Cost Analysis?



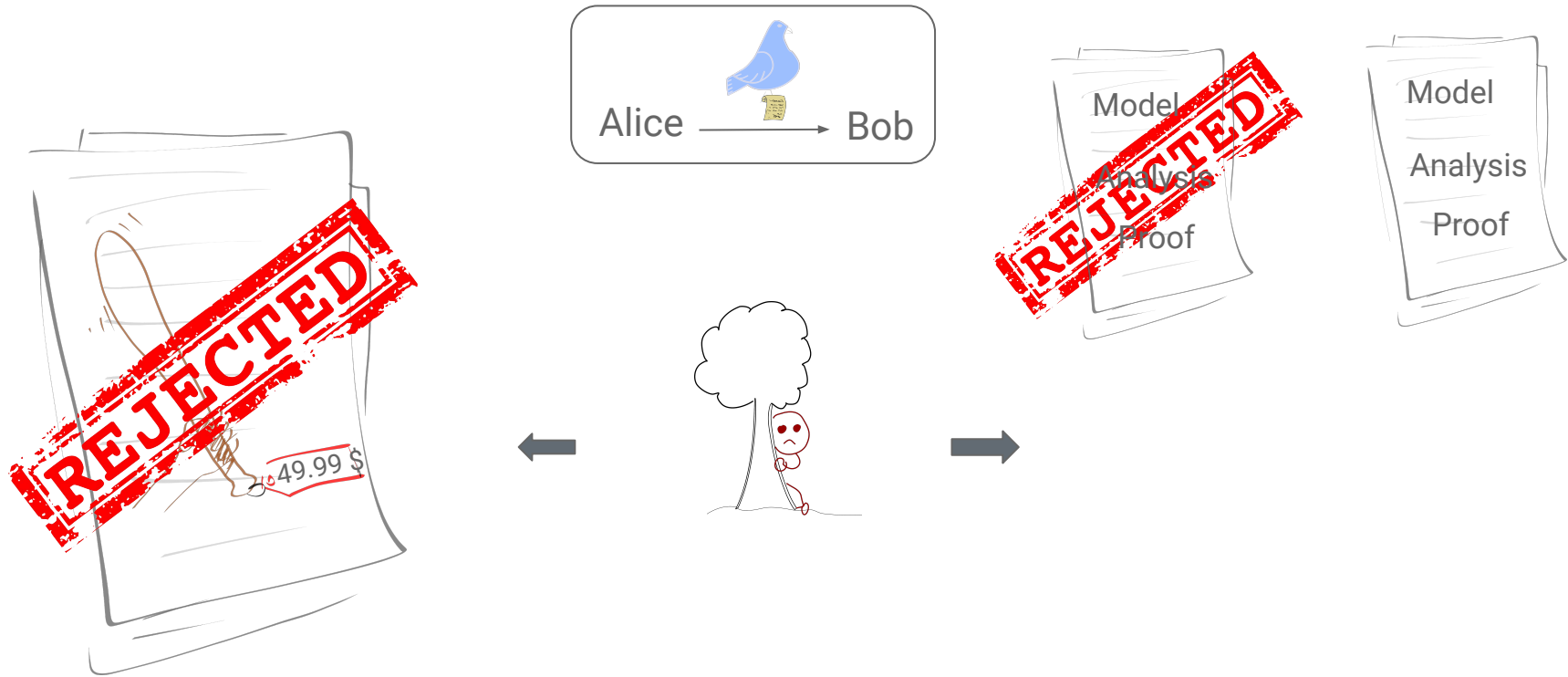
How to do a Cost Analysis?



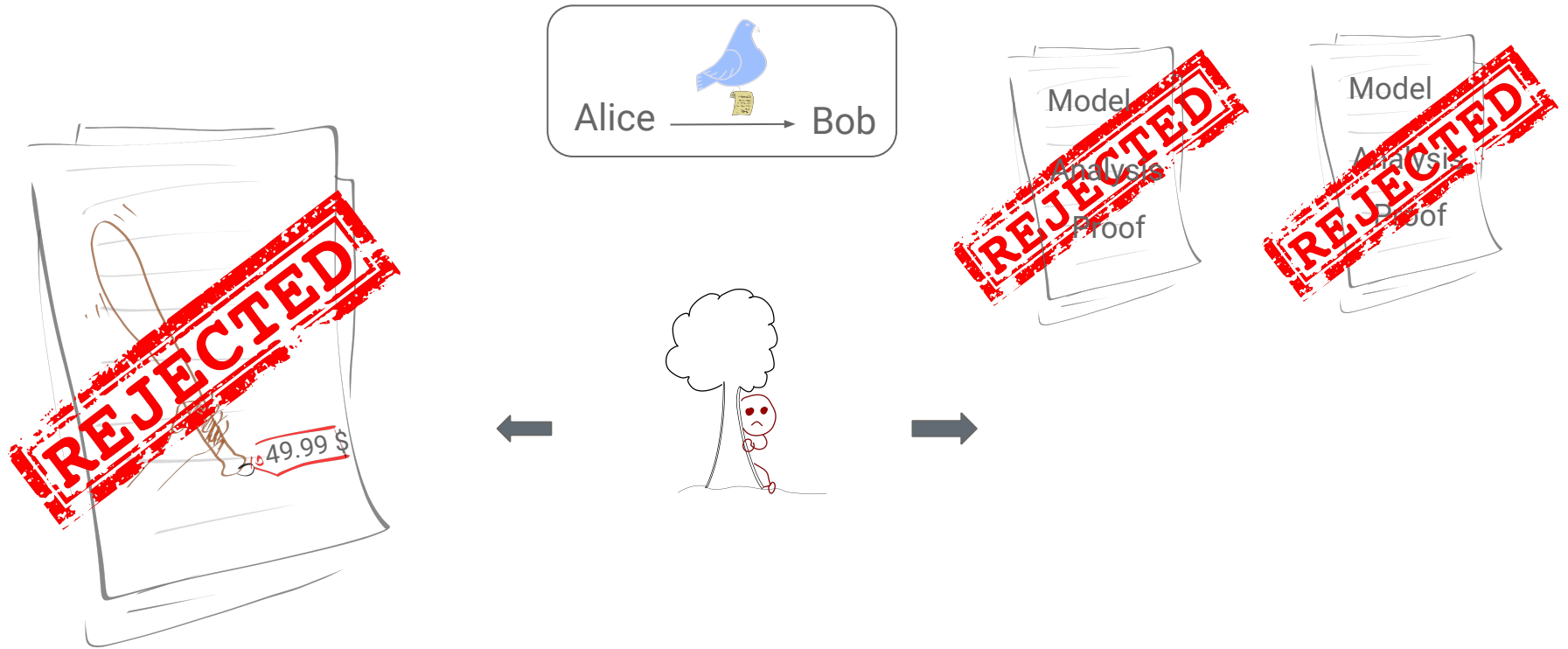
How to do a Cost Analysis?



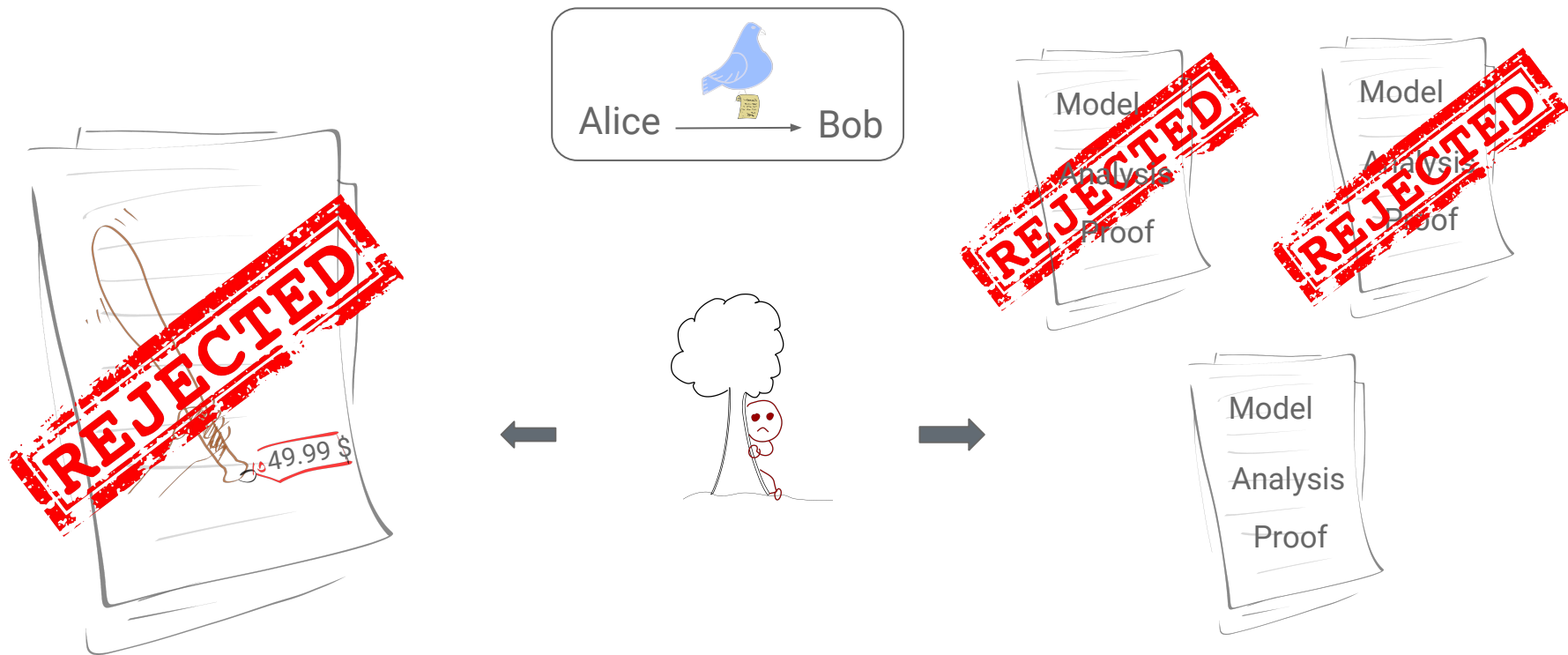
How to do a Cost Analysis?



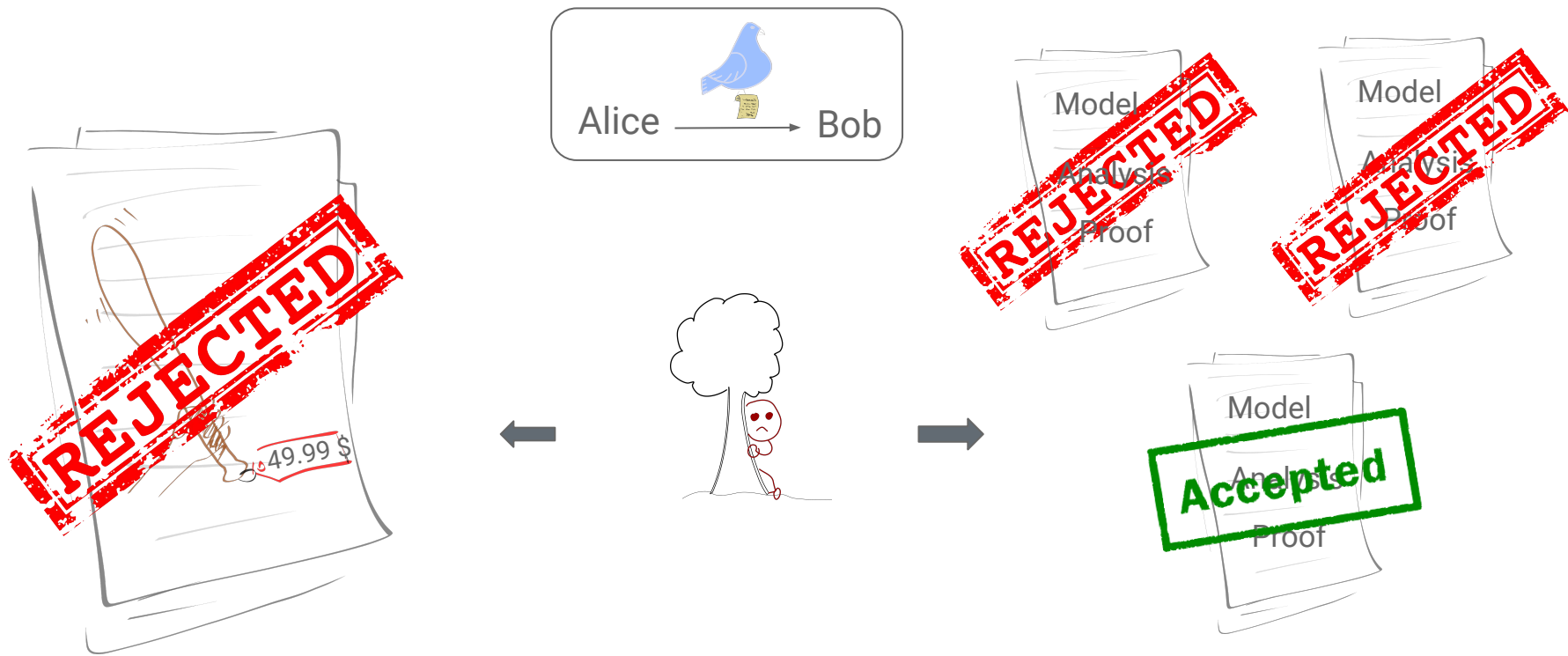
How to do a Cost Analysis?



How to do a Cost Analysis?



How to do a Cost Analysis?



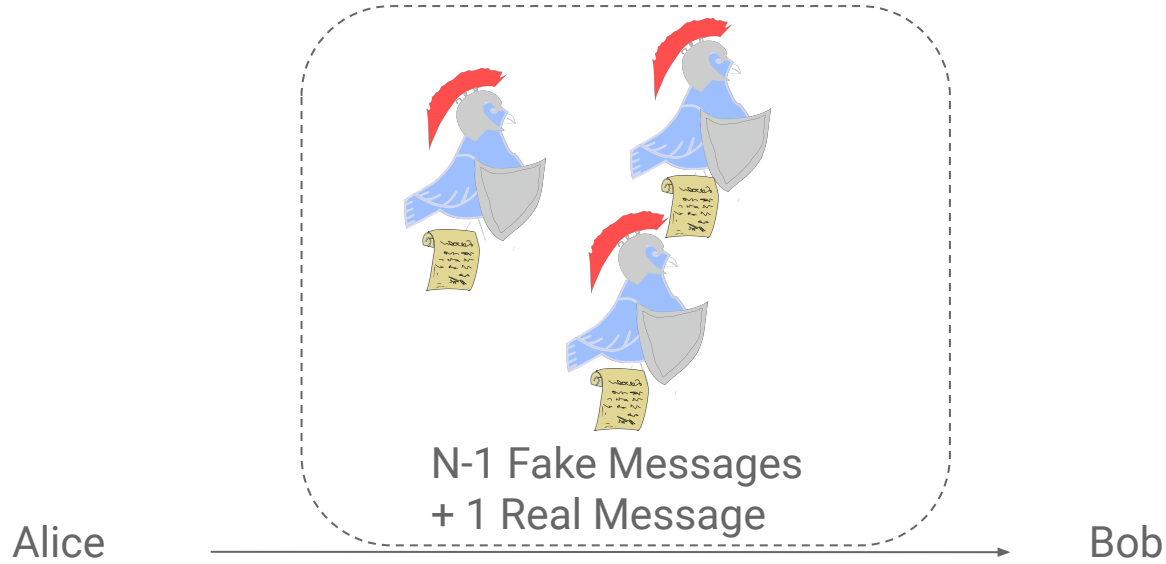
Secure Pigeon Protocol

Alice

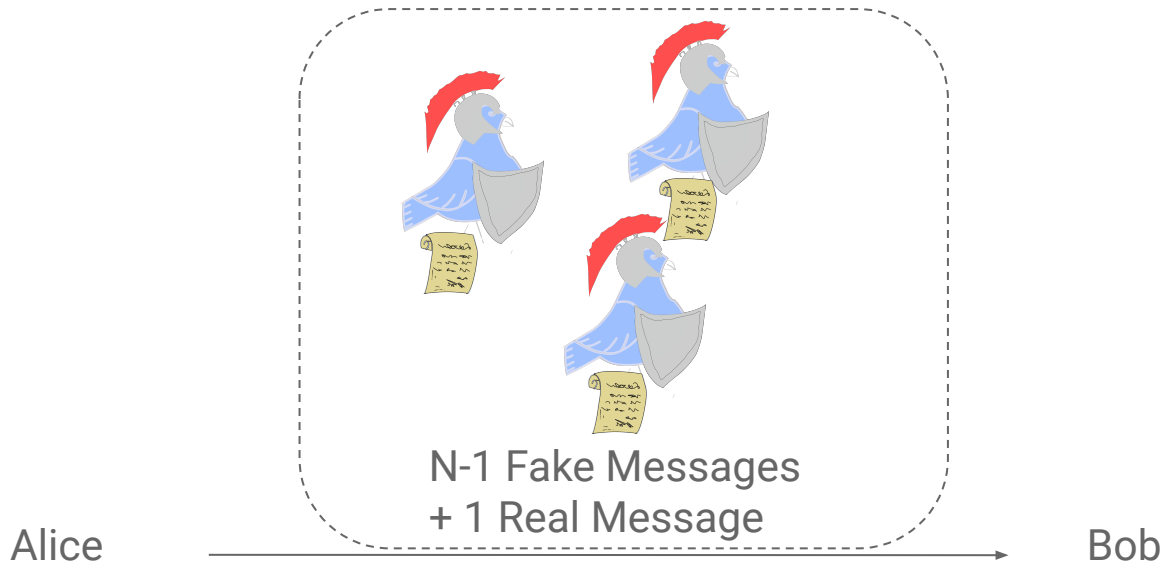


Bob

Secure Pigeon Protocol



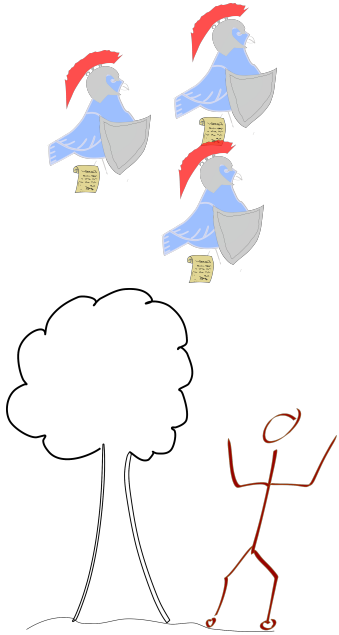
Secure Pigeon Protocol



Assumption: Pigeons Indistinguishable

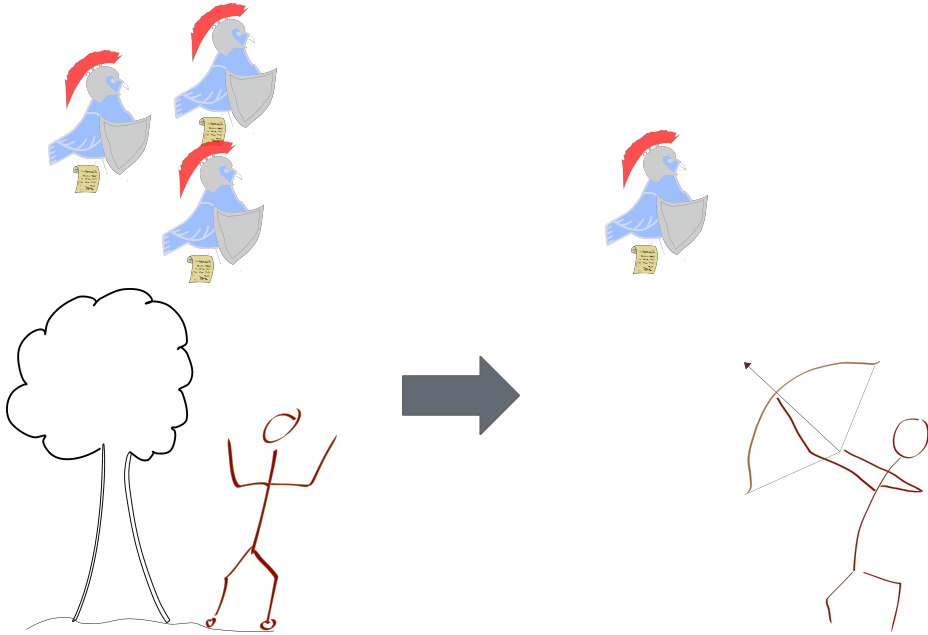
Indistinguishability under Chosen Pigeon Attack (IND-CPA)

Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons...

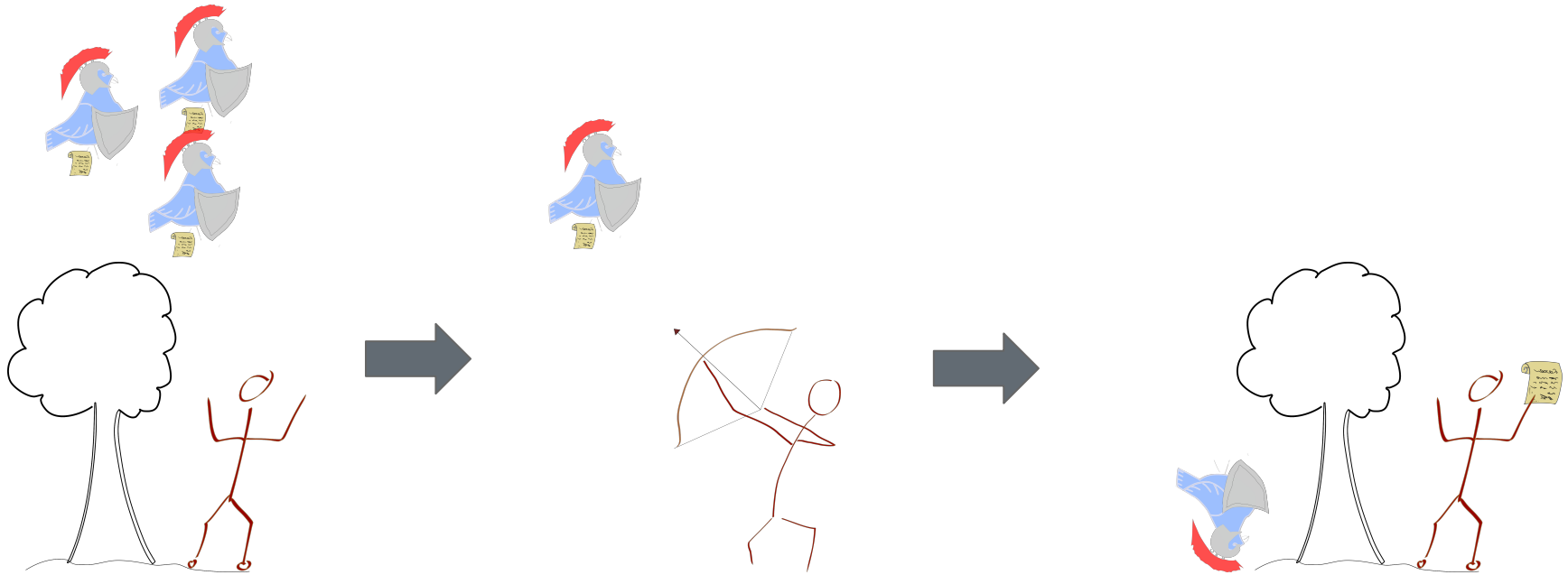
Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons...

... choose which to shoot ...

Indistinguishability under Chosen Pigeon Attack (IND-CPA)



Access to pigeons...

... choose which to shoot ...

... tell which message was real.

What is Eve's cost to find the real message?

Security Proof

Theorem:

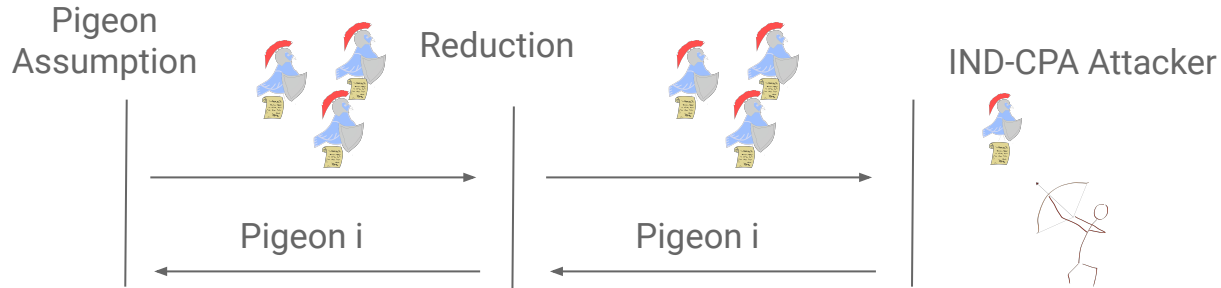
The protocol is secure, unless Eve can distinguish pigeons.

Security Proof

Theorem:

The protocol is secure, unless Eve can distinguish pigeons.

Proof:

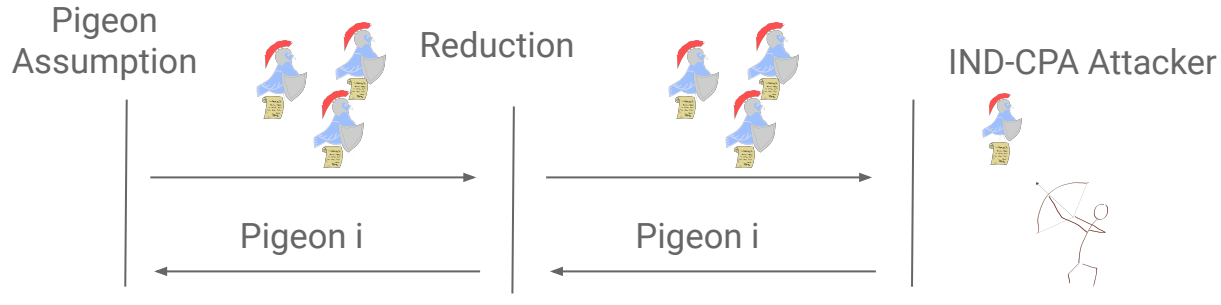


Security Proof

Theorem:

The protocol is secure, unless Eve can distinguish pigeons.

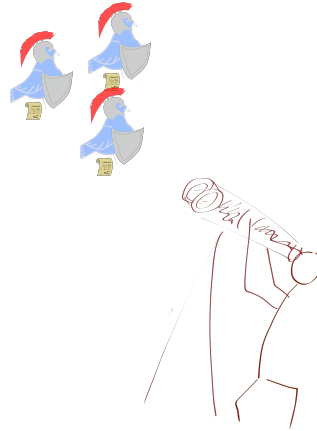
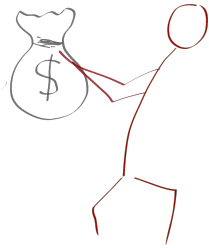
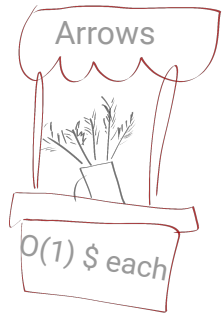
Proof:



Conclusion: \Rightarrow Need to shoot **$O(N)$** Pigeons.

So what is Eve's cost now?

Quantifying Security Costs



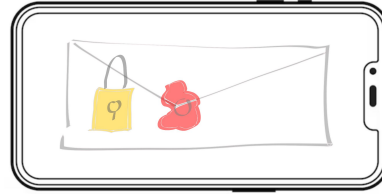
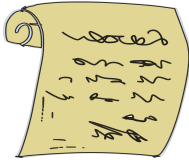
How expensive?

Best attack?

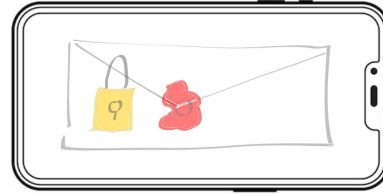
Feasibility?

Where do all the KASTEL pigeons
live?

Pigeons and Bows: A Future Perspective



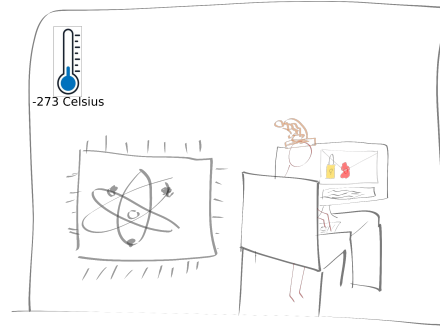
Pigeons and Bows: A Future Perspective



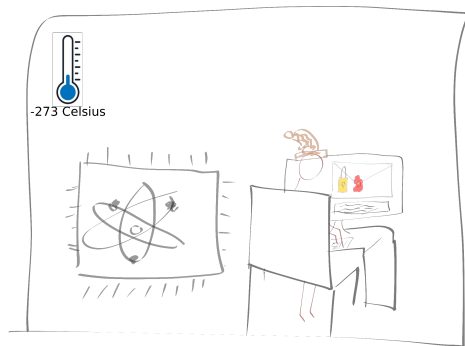
In the past





Future?



Intrigued?



Intrigued?

To promotionsgesprach@informatik.kit.edu , Marcel Tiepelt <marcel.tiepelt@kit.edu> 

Subject **Prof. Müller-Quade / "Costing Adversaries on Quantum-Secure Cryptography"**

Then invite me to a “Professorengespräch”!

