

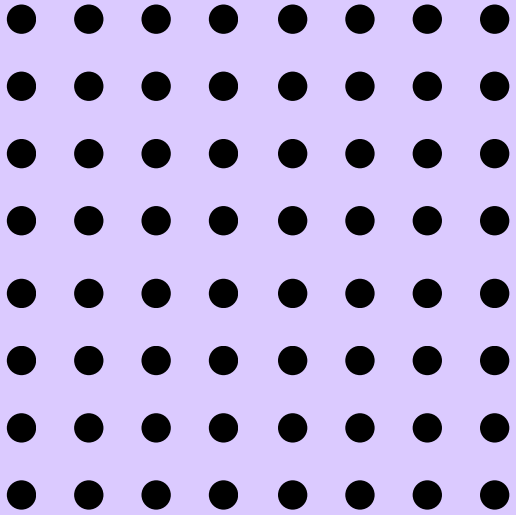
# On Sigma Protocols

Constructing the AND, OR Composition



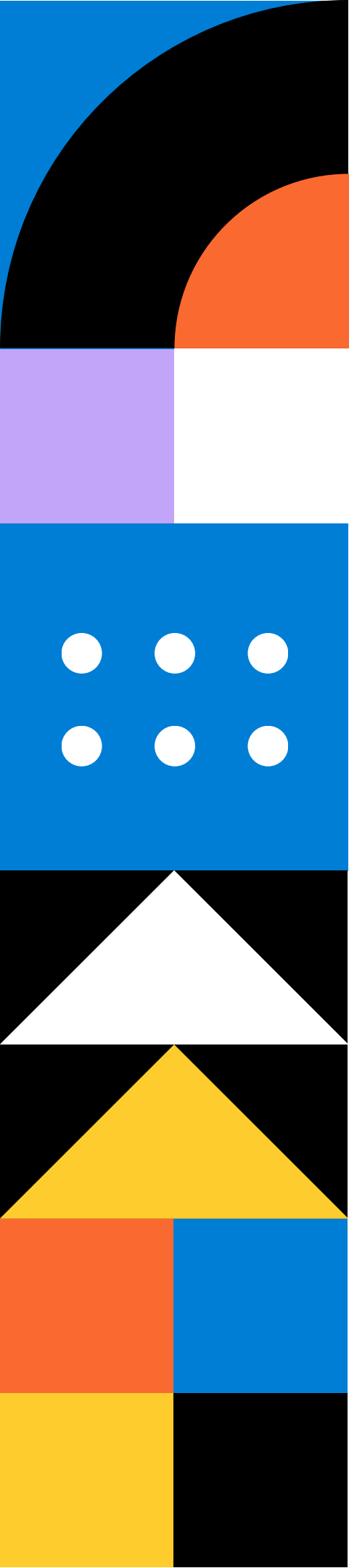
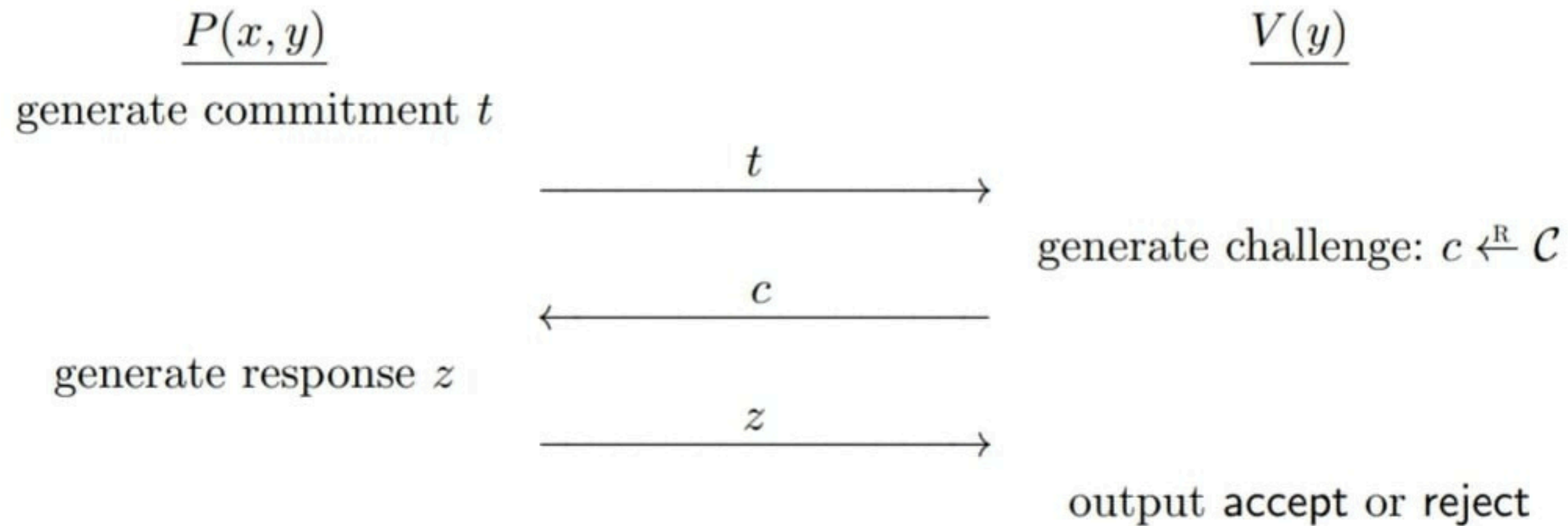


# What we shall cover

- 
- Definition of Sigma Protocols
  - Construction of AND Composition
  - Construction of OR Composition
  - Show that the constructions are valid



# Sigma Protocol Flow



# Sigma Protocols

Sigma Protocols provide a formal framework for realizing a Zero-Knowledge Proof (ZKP)

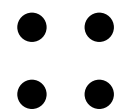
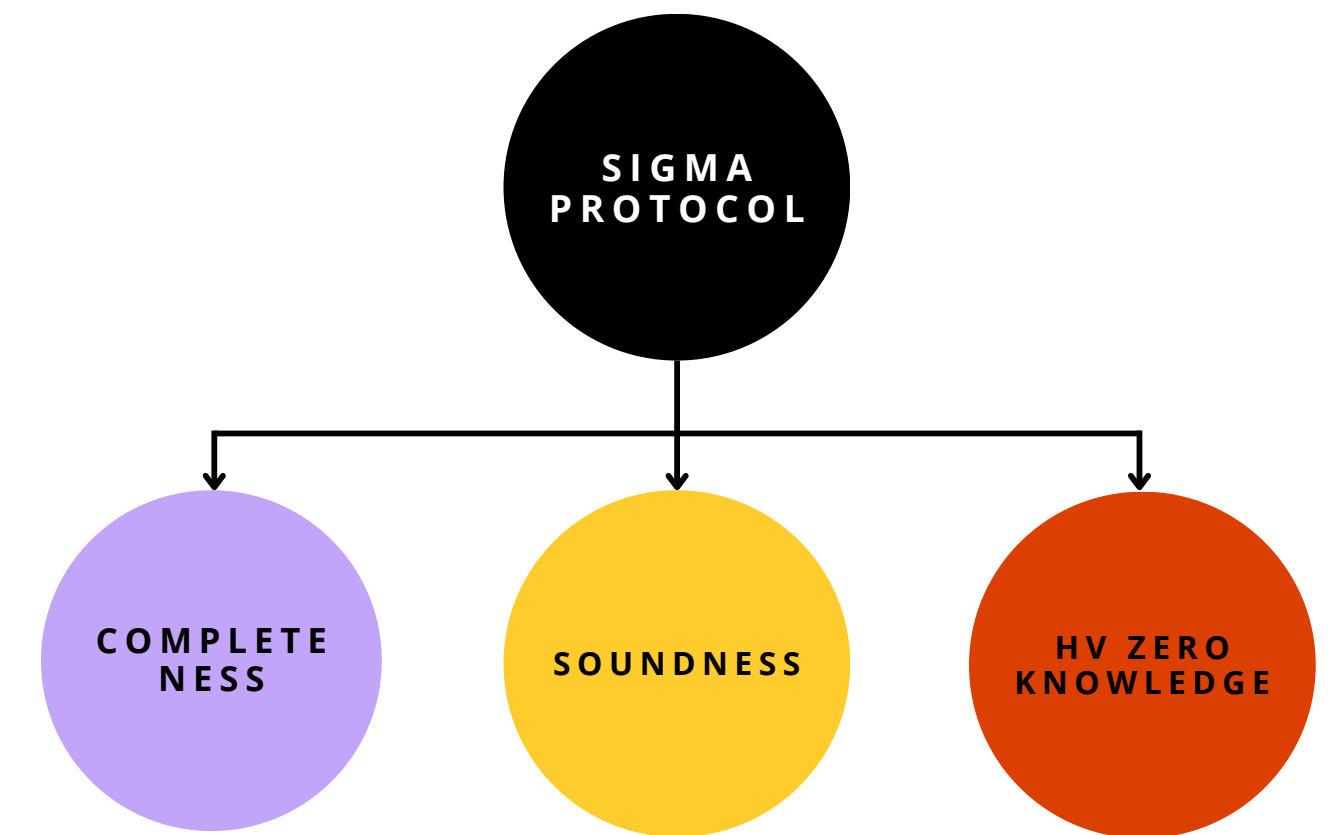
**Definition:** Given an effective binary relation  $R$  and let  $(x, y)$  be an element in  $R$  then for an interactive two-part protocol specified by algorithms  $(P, V)$  is a sigma protocol for  $R$  with challenge space  $C$  if the following hold:

- **Completeness:** The verifier  $V$  accepts all  $(x, y)$  if  $(x, y)$  belongs in  $R$ .
- **Special soundness:** There exists an efficient extractor for the witness  $x$  given two accepting transcripts and a statement  $y$
- **Special Honest Verifier Zero-Knowledge:** There exists an efficient simulator for the protocol such that the simulator outputs an accepting transcript for the protocol whenever invoked



# In Layman Terms

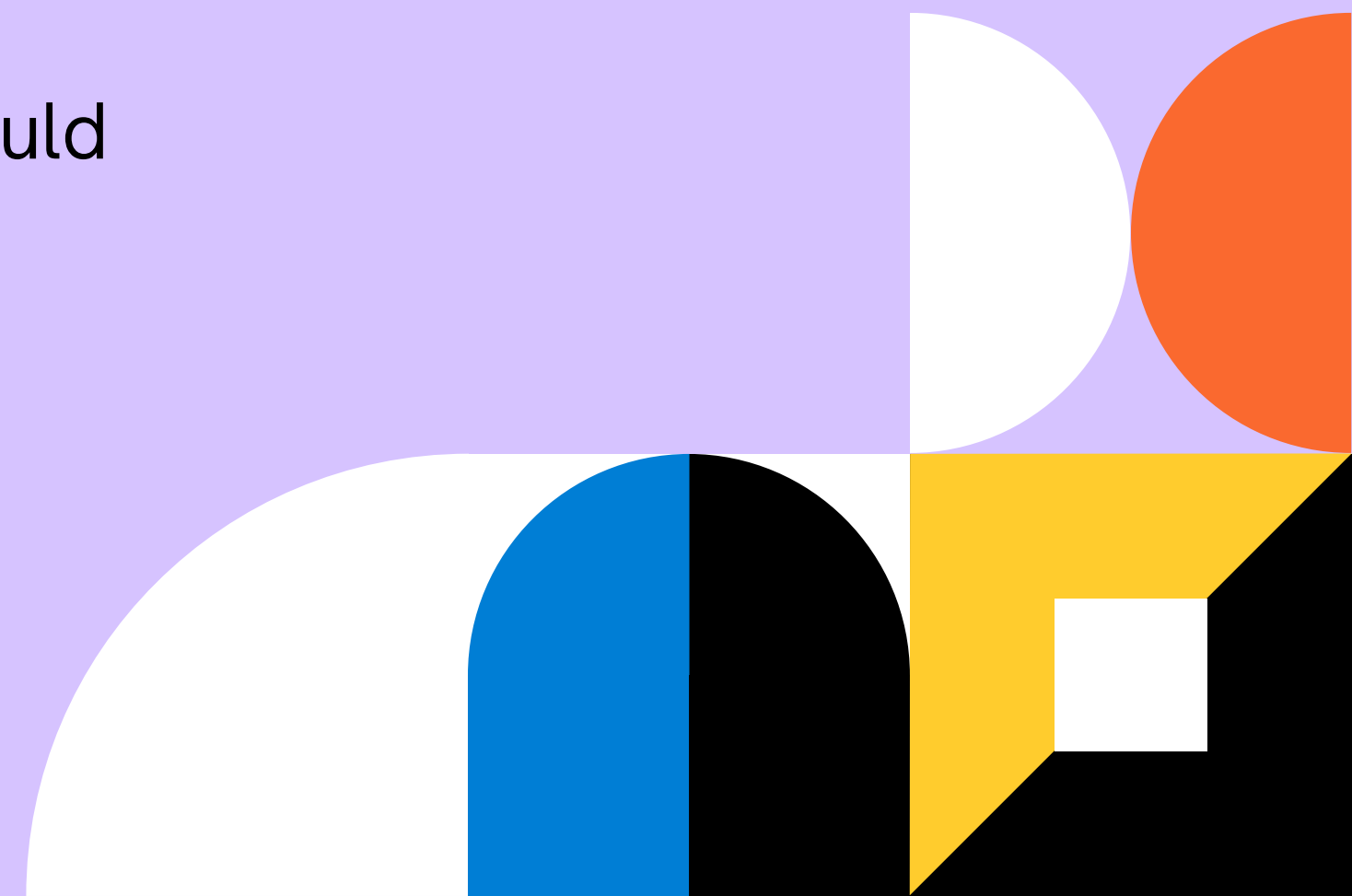
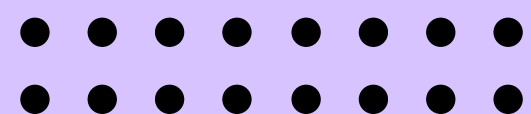
- **Completeness:** Someone who knows the witness can always convince the verifier.
- **Soundness:** The prover cannot fake knowing the witness to the verifier.
- **HVZK:** If the verifier follows the protocol honestly then the verifier receives no additional information about the witness.





# Re: Story of Ali-Baba

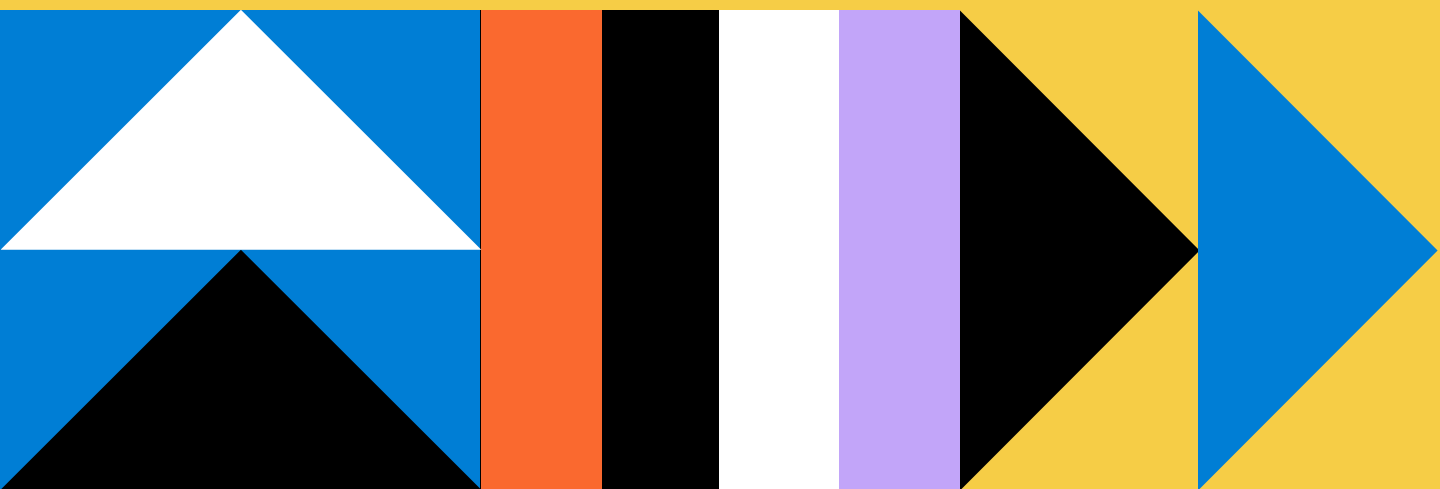
- To prove to the journalist that Ali-Baba knew the magic word, he first entered the cave from an arbitrary direction, which was unknown to the journalist.
- He then comes out from the side the journalist would call out. Doing this many times would prove to the journalist that Ali-Baba knew the secret word.





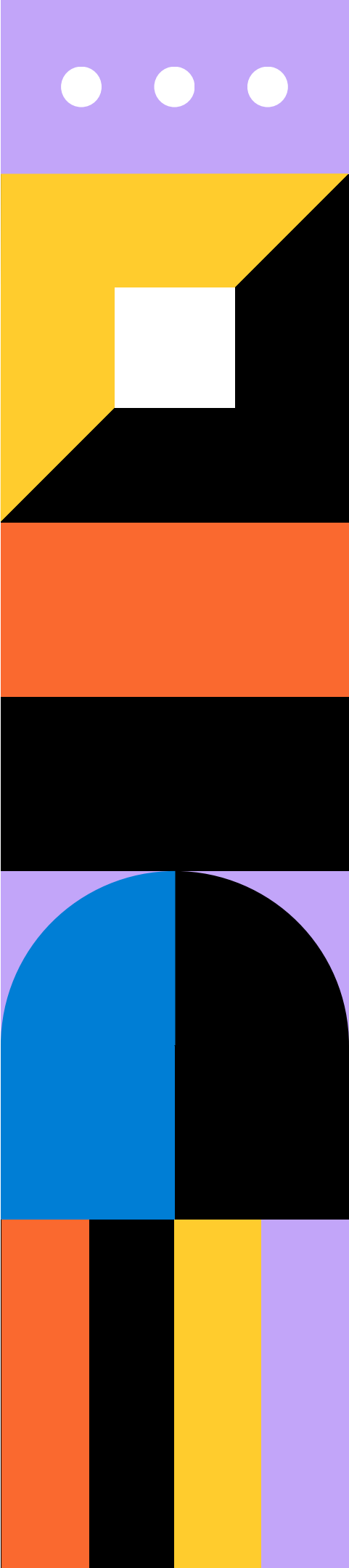
# AND Protocol

Many years later, a journalist decides to interview Ali-Baba's descendants, Calvin and Hobbes, about the magic cave. The two claimed to know the secret phrase of the cave but refused to reveal it. The journalist wanted to verify this but couldn't interview each of them separately as he had a flight to catch. How do you resolve this situation?

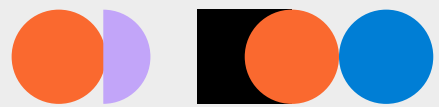


# Verify at the same time !!

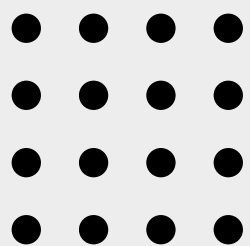
- Calvin and Hobbes walk into the cave, and each independently chooses the entrance route.
- The journalist then flips a coin and asks both of them to exit from the right if the coin lands on heads or else exit from the left.
- Repeating this many times would show that both of them must know the secret phrase.
- If the journalist played along honestly then he received no additional information about the secret phrase.
- This forms the basis of the AND composition of 2 sigma protocols.







# AND Composition

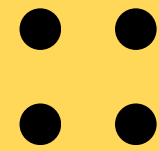


The AND composition allows a prover to convince a verifier that he knows the witnesses to 2 statements at the same time.

The protocol essentially relies on computing the responses for each of the base protocols separately.



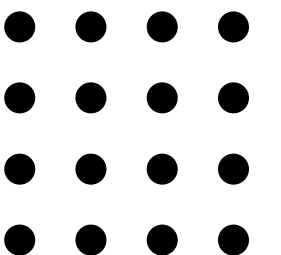
# AND Composition



**Construction:** We can construct a sigma protocol for the following relation:

$$R = \{(x_0, x_1, y_0, y_1) \mid (x_0, y_0) \in R_0 \wedge (x_1, y_1) \in R_1\}$$

- Prover receives the input and computes the output commitments for each base protocol.
- The verifier then chooses a challenge and sends it to the prover.
- The outputs are then computed for each base protocol and sent to the verifier.
- The verifier accepts if and only if each transcript is accepted by the base verifier of each protocol

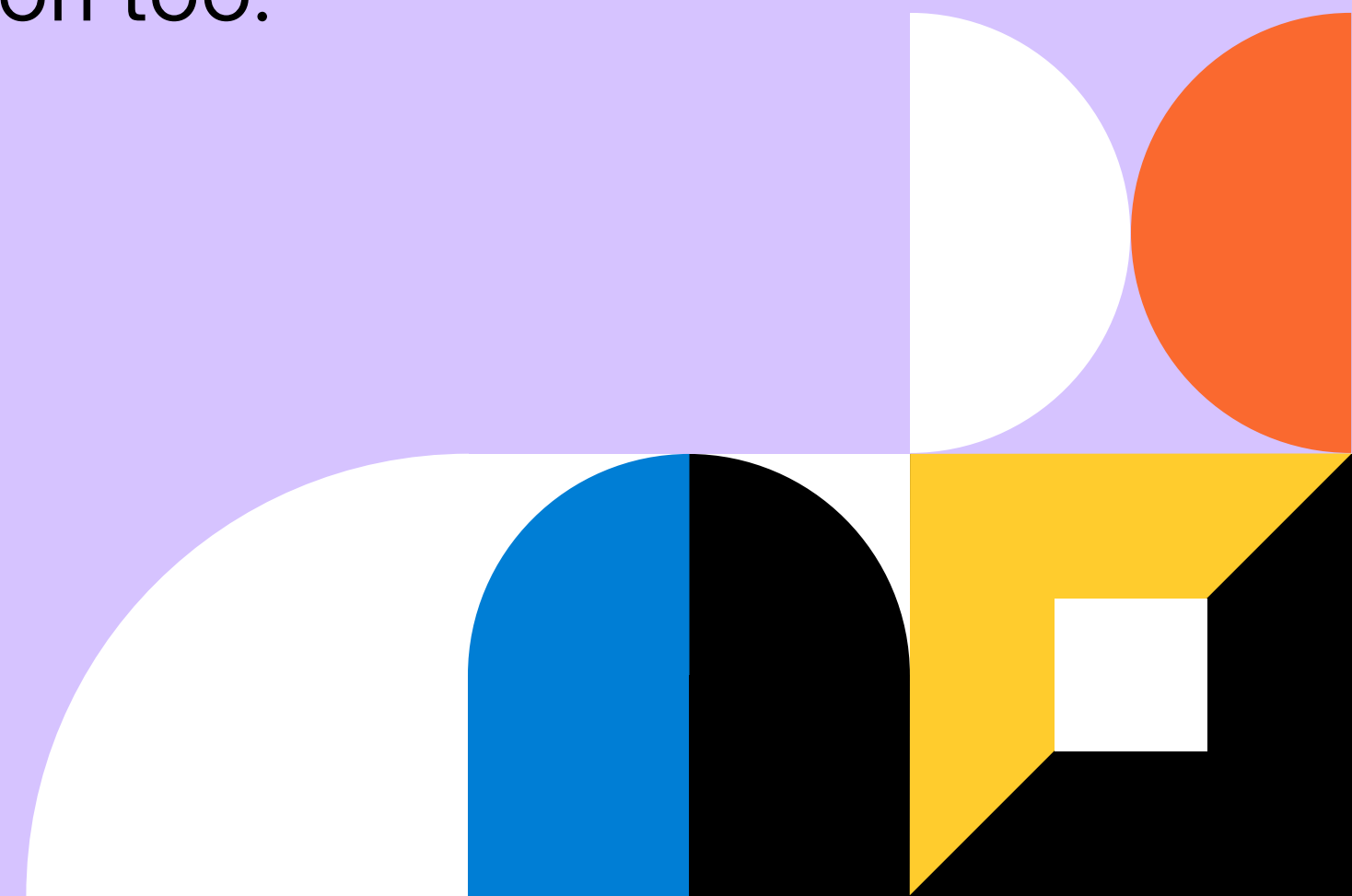
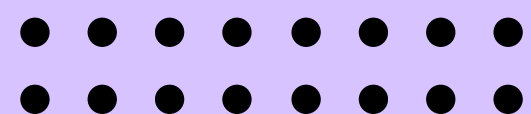




# Proof of Completeness

Since Calvin and Hobbes both know the password, each of them can individually convince the verifier and hence they can convince the verifier for the given construction too.

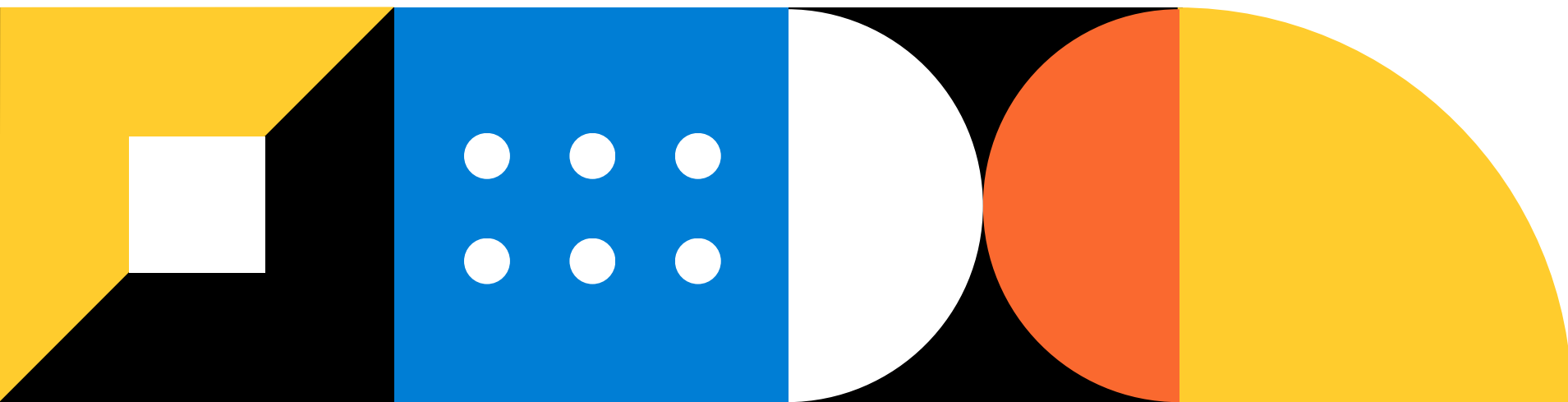
This shows that the protocol is complete.

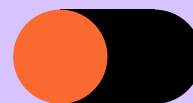




# Proof of Soundness

Calvin and Hobbes are able to convince the verifier since both of them know the password. If one of them didn't know the password then they would fail the test if they entered the cave from the opposite direction as the one announced.

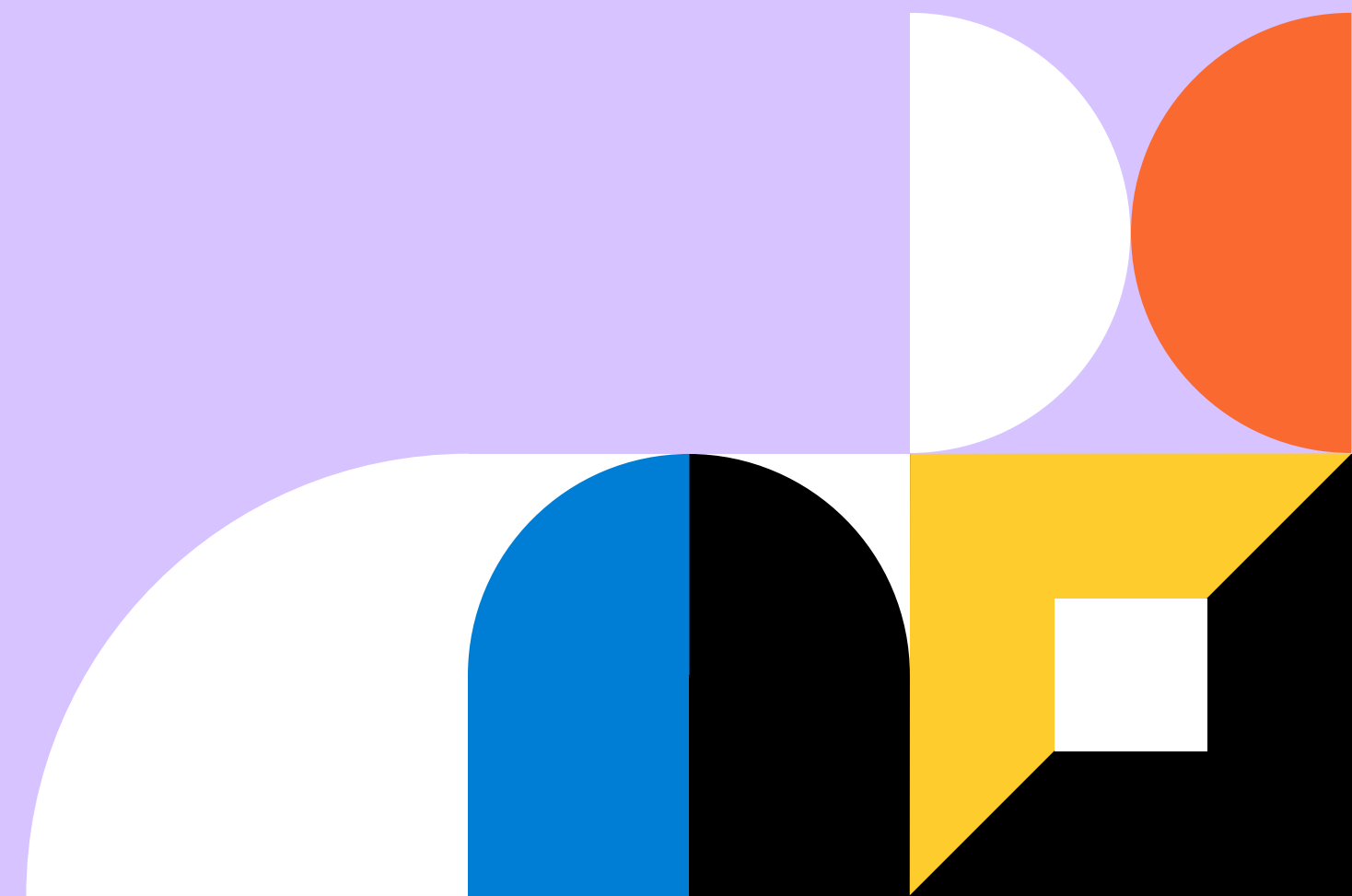
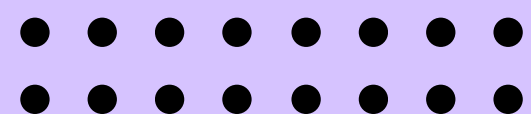




# Proof of HVZK

Since the verifier isn't malicious and doesn't accompany any of them into the cave, he can't possibly know the password.

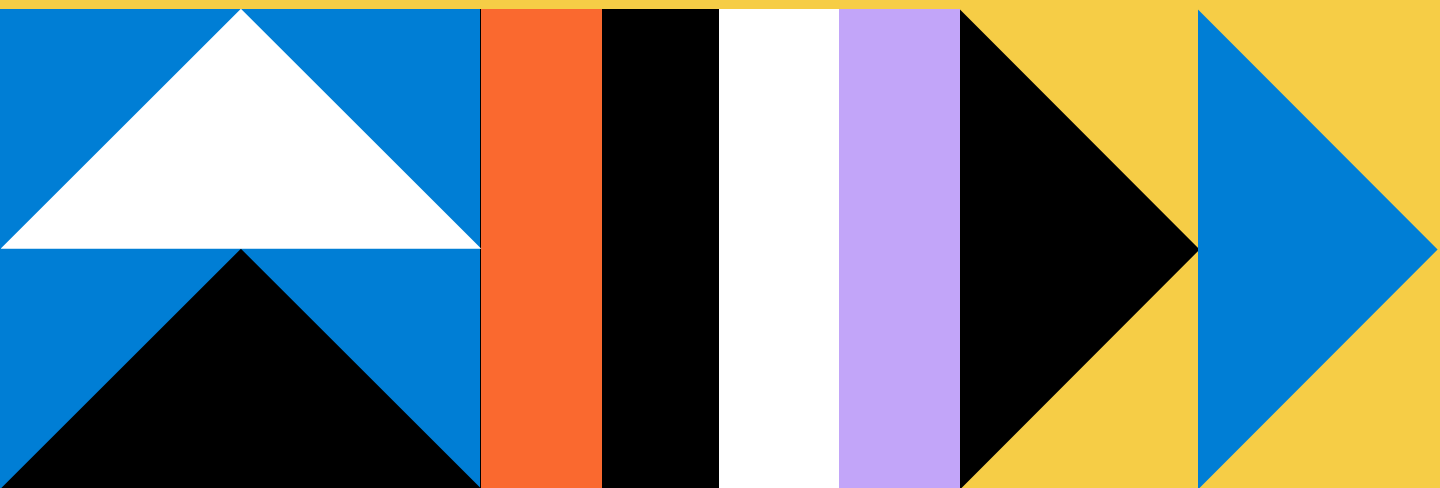
This proves HVZK.





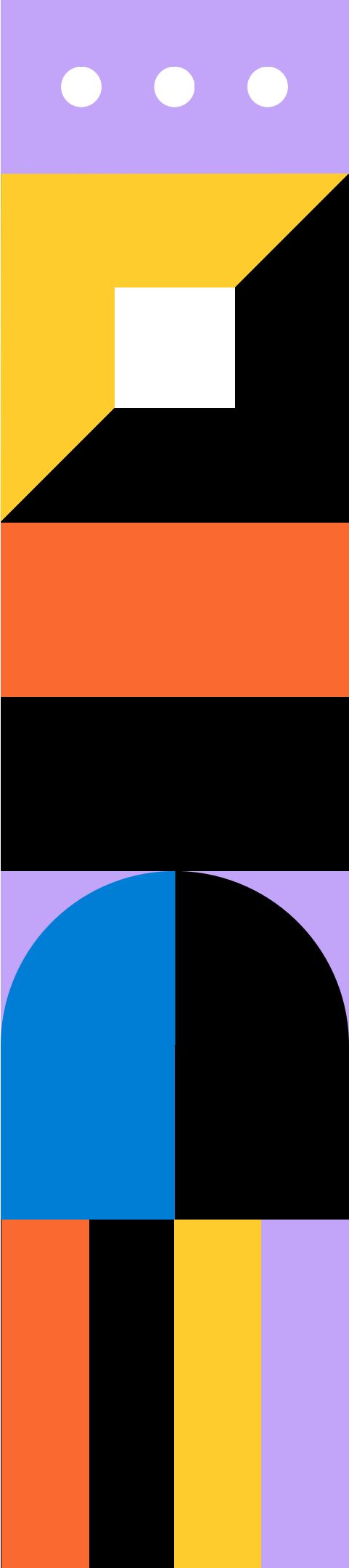
# OR Protocol

Another pair of Alibaba's descendants, Luke and Leia, claimed that at least one of them knew the password to the cave (Leia had amnesia and forgot the password over the years but the journalist doesn't know that). The journalist wanted to verify this but couldn't interview each of them separately as he had a flight to catch. How do you resolve this situation?



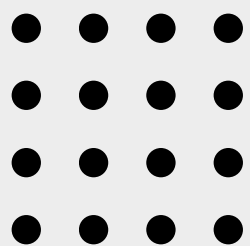
# Leia follows Luke!!

- Luke and Leia walk into the cave, but this time such that both of them go in the same direction.
- The journalist then flips a coin and asks both of them to exit from the right if the coin lands on heads or else exit from the left.
- Leia accompanies Luke every time the gate needs to be opened.
- Repeating this many times would show that at least one of them knows the secret but won't reveal which one knows.
- If the journalist played along honestly then he received no additional information about the secret phrase or who knew the secret.
- This forms the basis of the OR composition of 2 sigma protocols.





# OR Composition



The OR composition allows a prover to convince a verifier that he knows the witness to at least one of the 2 statements without revealing which one.

The protocol essentially relies on computing the response for the base protocol whose witness is known and simulating the response for the other.



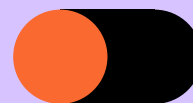


# OR Composition

**Construction:** We can construct a sigma protocol for the following relation:

$$R = \{(b, x, y_0, y_1) \mid (x, y_b) \in R_b\}$$

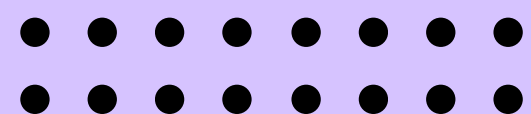
- Prover receives the input and computes the output commitments by simulating the unknown relation for an arbitrary challenge and computing it for the known relation.
- The verifier then chooses a challenge and sends it to the prover.
- The outputs are then computed for the known relation using an encoded challenge.
- The verifier accepts if and only if each transcript is accepted by the base verifier of each protocol



# Proof of Completeness

Since at least one of Luke and Leia (Luke here), know the secret to the cave, both of them can come out from the announced direction.

This proves completeness.

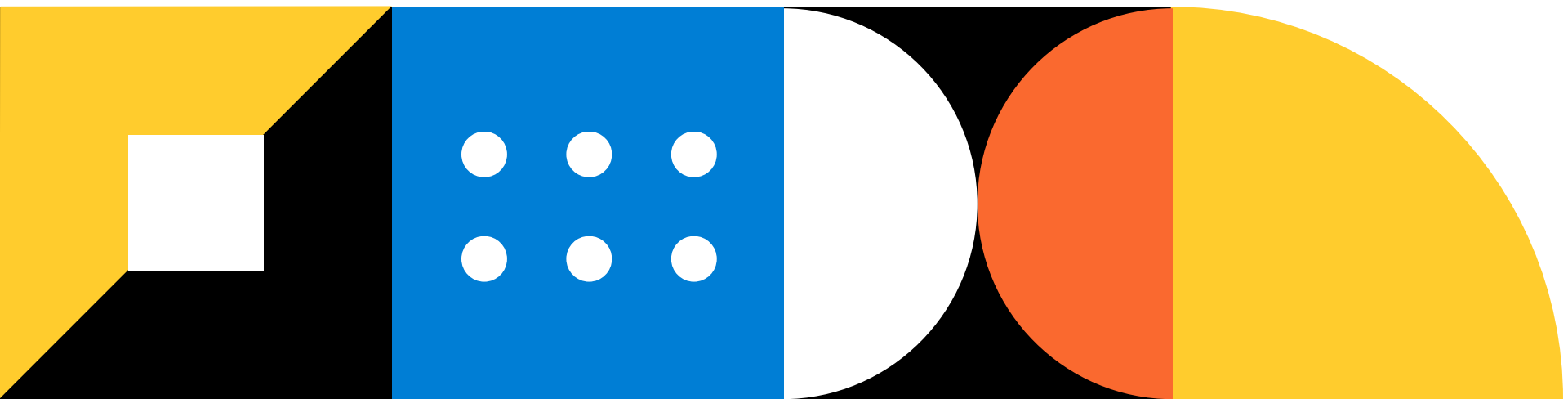




# Proof of Soundness

If neither of the two knew the password, they wouldn't always be able to come out from the announced direction.

This proves soundness.

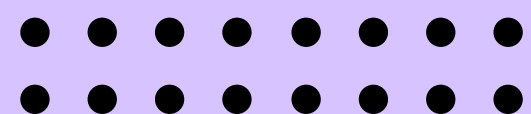




# Proof of HVZK

Since the verifier isn't malicious and doesn't accompany any of them into the cave, he can't possibly know the password as well as the person who uses the password.

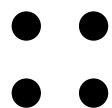
This proves HVZK.





# References

1. 'A Graduate Course in Applied Cryptography' -  
Dan Boneh, Victor Shoup, Version 6, 2023





Thank You

