EXPLORING CRYPTOGRAPHY PROTOCOLS

WITH LIMITED EMPHASIS ON MATHEMATICS ☺

Presented By
@7eRoM

ATTENTION

THESE SLIDES HAVE BEEN CRAFTED USING THE FOUNDATION OF MY MSC COURSE IN CRYPTOGRAPHY PROTOCOLS AT THE UNIVERSITY OF ISFAHAN.

I'VE MADE ADJUSTMENTS TO THE CONTENT TO ALIGN WITH THE SPECIFIC OBJECTIVES OF THIS PRESENTATION.

ALSO, MY INTENTION HAS BEEN TO MINIMIZE THE USE OF MATHEMATICAL CONCEPTS, WHICH MAY RESULT IN SOME CONCEPTS BEING SIMPLIFIED OR LESS PRECISE.

Agenda

1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. Threshold Cryptography and Secret Sharing Protocols
5. Types of Digital Signatures
6. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
7. Identity Based Cryptography
8. Secure Auctions and Elections Protocols
9. Cryptocurrency
10. Secure Multiparty Computations

Agenda

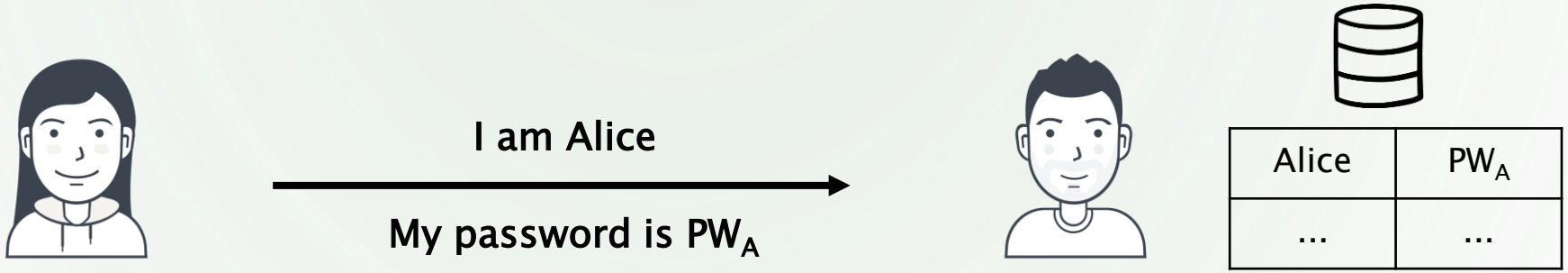
1. Identification and Entity Authentications Protocols
2. Zero Knowledge Protocols
3. Key Establishment Protocols
4. Threshold Cryptography and Secret Sharing Protocols
5. Types of Digital Signatures
6. Special Purpose Protocols (like simultaneous contract signing, mental poker, fair exchange)
7. Identity Based Cryptography
8. Secure Auctions and Elections Protocols
9. Cryptocurrency
10. Secure Multiparty Computations

Levels of Authentications

- Weak Authentication (based on password)
- Strong Authentication (based on challenge and response)
- Extremely Strong Authentication (based on zero knowledge)

Weak Authentication

Protocol #1



Eavesdropping and Replay Attack

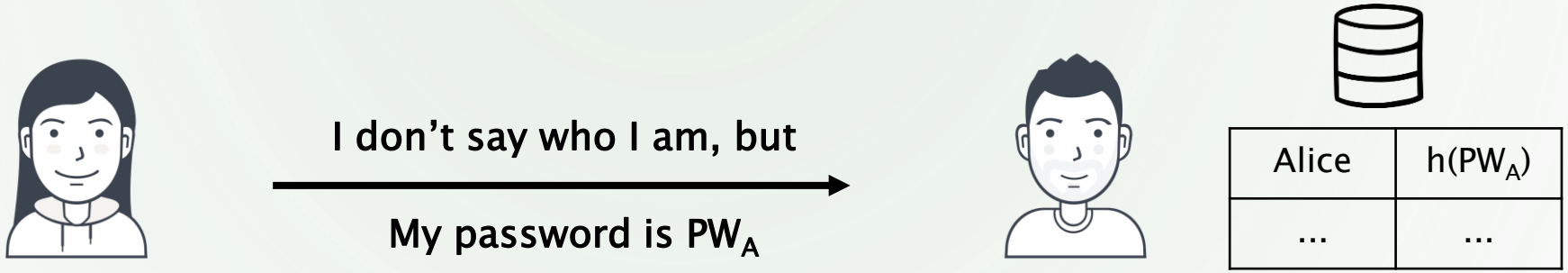
Unauthorized Access to DB

Dictionary Attack

Bob Knows Alice's Password

Weak Authentication

Protocol #2



Map Hash of Password to a User with Complexity of n/2

Birthday Attack to Find each PW

Weak Authentication

Protocol #3

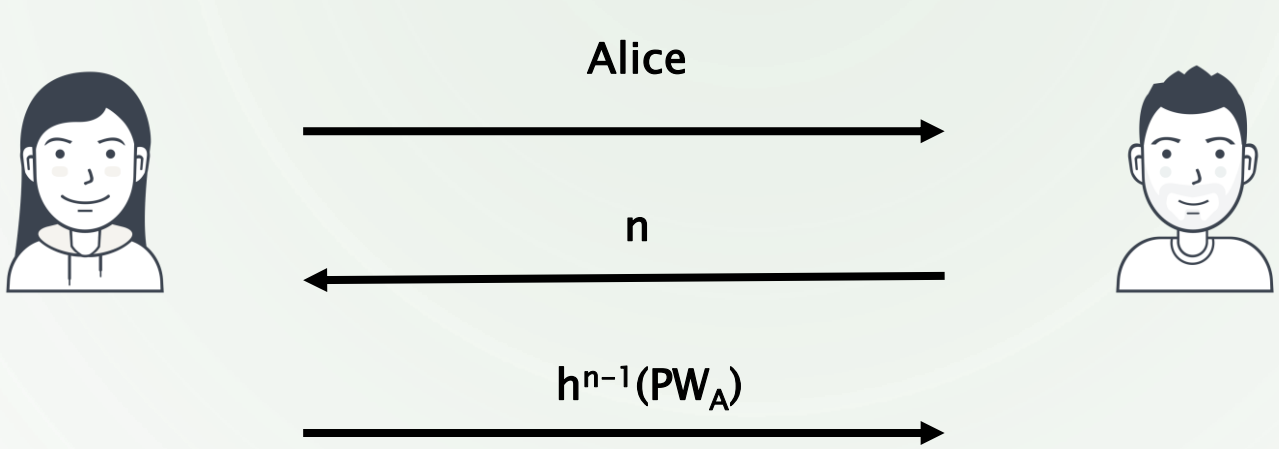
I don’t say who I am, but

My password is PW_A

Alice	$h(PW_A \| salt_A)$	$salt_A$
...	...	...

Weak Authentication

Lamport



user	next challenge	hash
Alice	n	$h^n(PW_A)$

Weak Authentication

Lamport

Alice →

← n

$h^{n-1}(PW_A)$ →

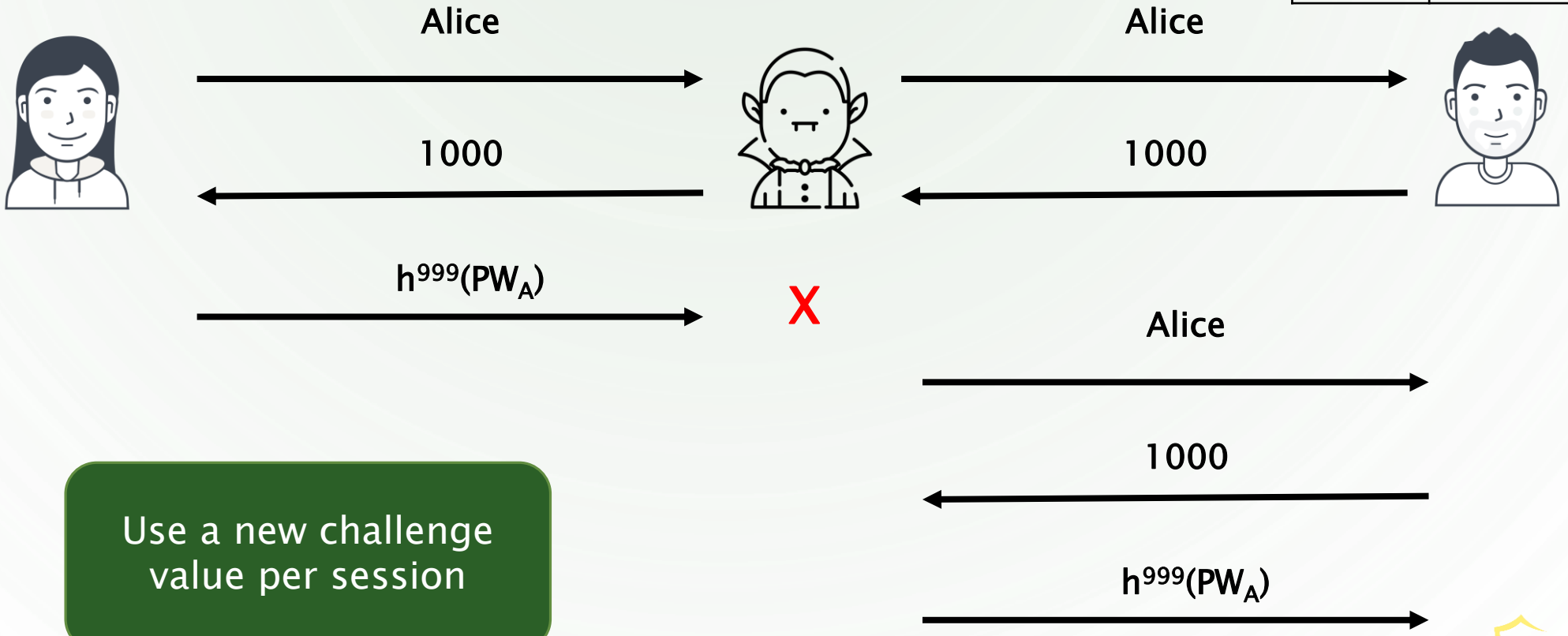
user	next challenge	hash
Alice	$n-1$	$h^{n-1}(PW_A)$

Why do we need to store the value of "n"?

Weak Authentication

Lamport

user	hash
Alice	$h^{1000}(PW_A)$

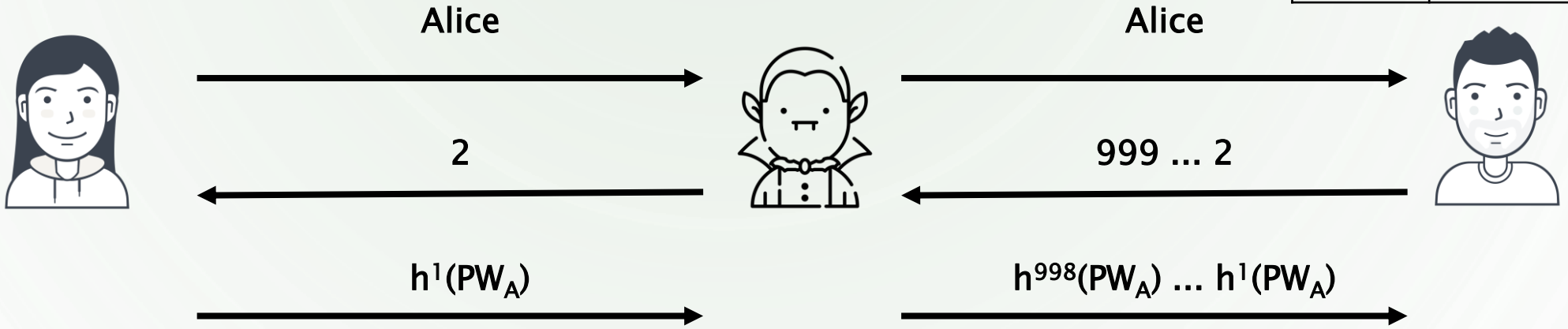


Use a new challenge value per session

Weak Authentication

Lamport (Small n Attack)

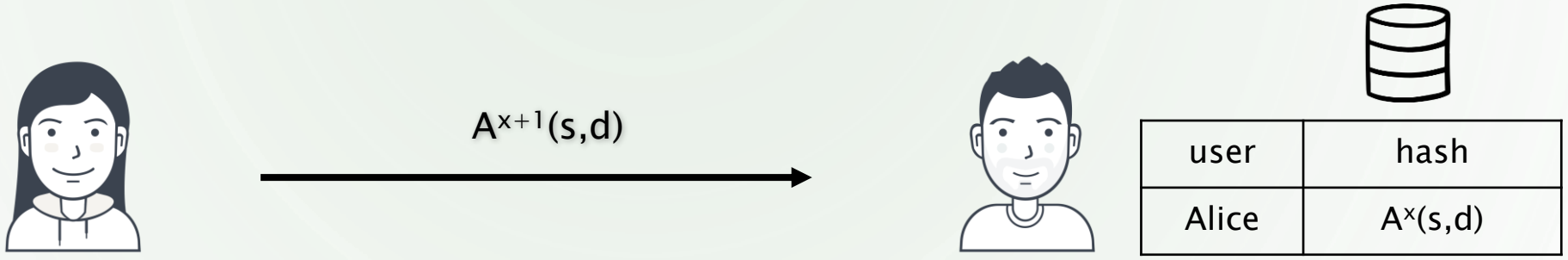
user	hash
Alice	$h^{1000}(PW_A)$



Alice must store the latest value of “n”

Weak Authentication

Infinite Length Hash Chain (ILHC)



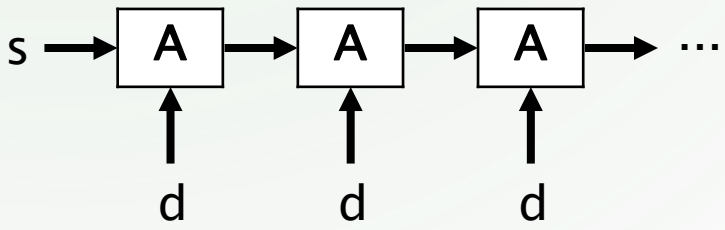
A -> Algorithm

d -> Private Key

e -> Public Key

s -> Paintext

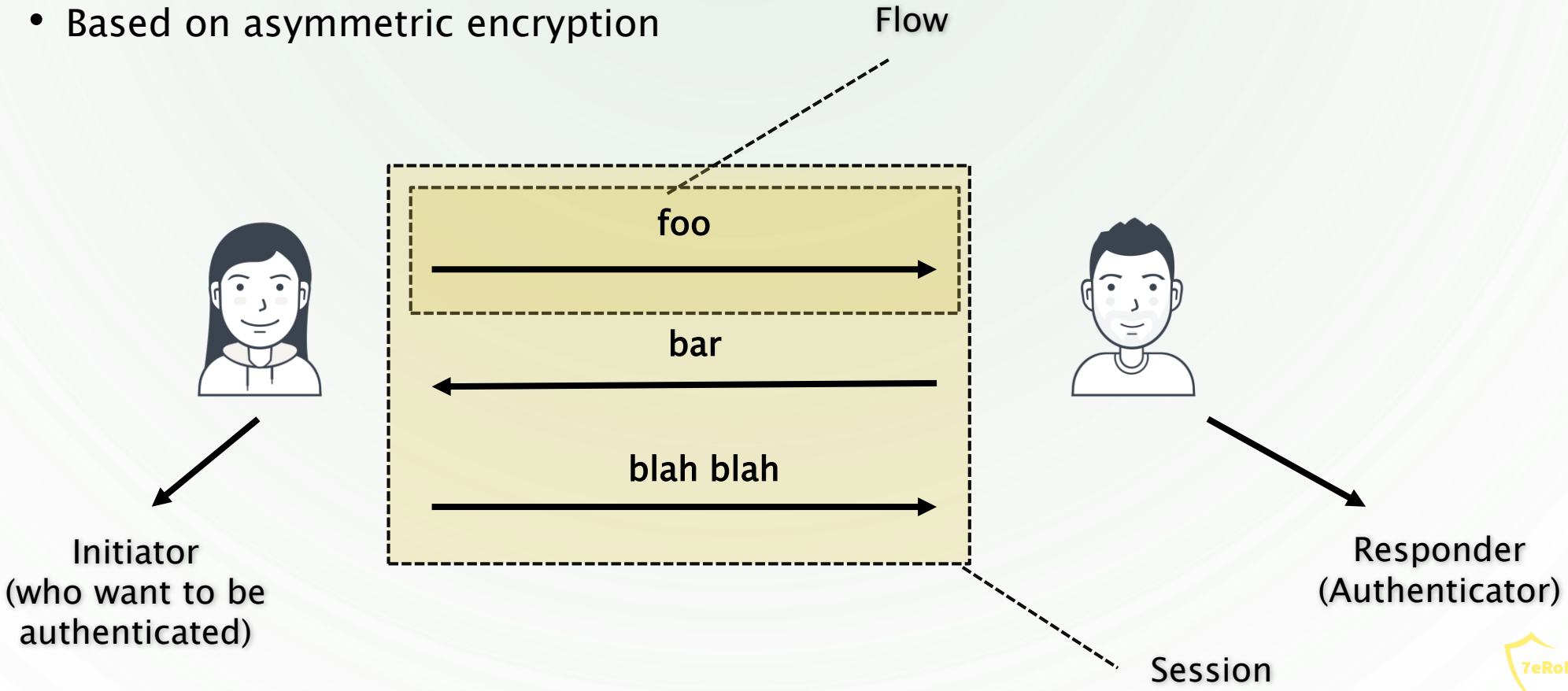
c -> Ciphertext



$s , A(s,d) , A^2(s,d) , \ldots , A^n(s,d) , \ldots$

Strong Authentications

- Types of Strong Authentications:
  - Based on symmetric encryption
  - Based on asymmetric encryption



Strong Authentication

Protocol #1

$MAC_K(.)$

request for authentication →

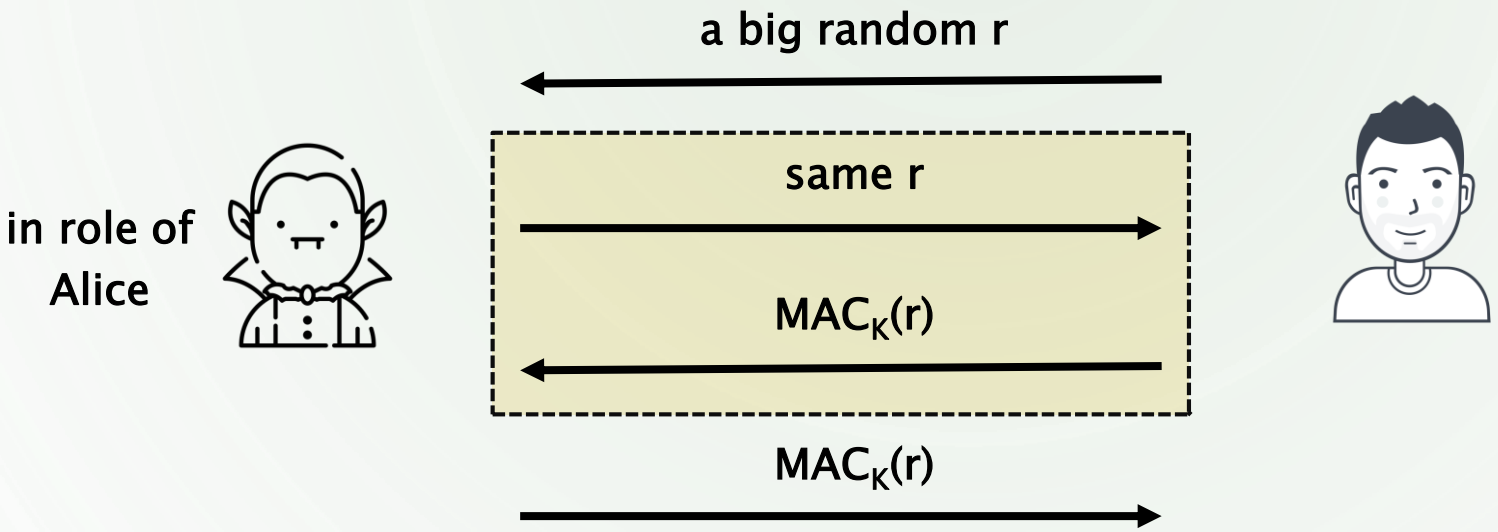
← a big random r

$MAC_K(r)$ →

$MAC_K(.)$

Strong Authentication

Parallel Session Attack



Suppose both Alice and Bob could be authenticator and could be authenticated as well

Strong Authentication

Protocol #2

$MAC_K(.)$

request for authentication →

← a big random r

$MAC_K(A \mid r)$ →

$MAC_K(.)$

Strong Authentications

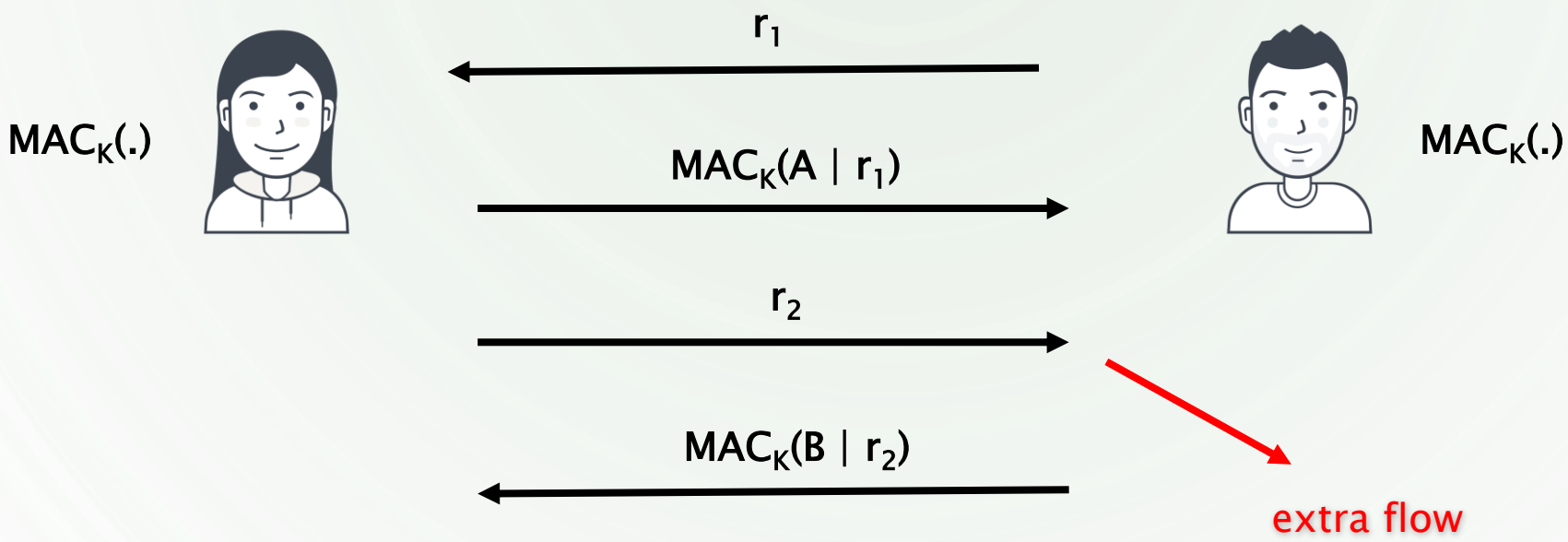
Mutual Authentication or Bilateral Authentication

- Both Alice and Bob can authenticate each other

- Two conditions of scheme:
  - **Completeness:** If both Alice and Bob are honest and the enemy is passive, the result of session must be pass by both.
  - **Soundness:** If the enemy got involved in just a flow or more, the result of session must be fail by both.

Strong Authentication

Protocol #3



Strong Authentication

Protocol #4

$MAC_K(.)$

r_1

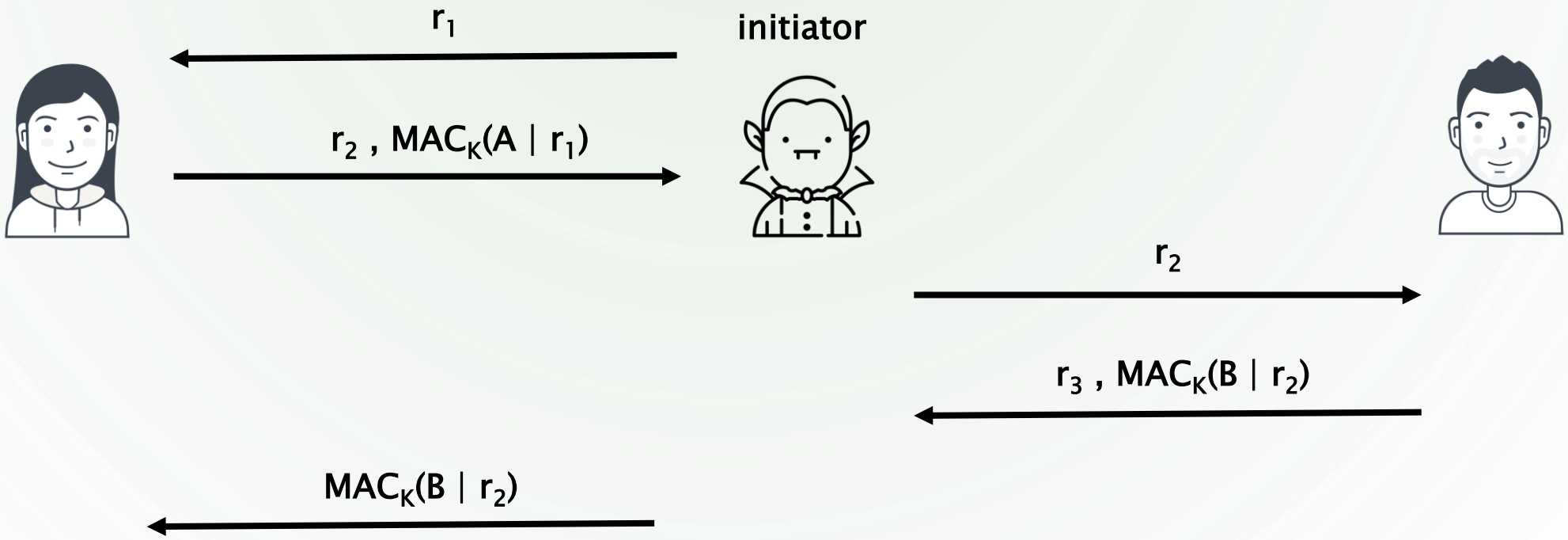
r_2 , $MAC_K(A \mid r_1)$

$MAC_K(B \mid r_2)$

$MAC_K(.)$

Strong Authentication

Parallel Session Attack



Strong Authentication

Protocol #5

$MAC_K(.)$

r_1

r_2 , $MAC_K(A \mid r_1 \mid r_2)$

$MAC_K(B \mid r_2)$

$MAC_K(.)$

Strong Authentication

Asymmetric Encryption

TA	Trusted Authority
CA	Certificate Authority
PK_A	A's Public Key
PR_A	A's Private Key
$sig_A(x)$	Encrypt x by A's Private Key
$ver_A(x, y)$	Decrypt y by A's Public Key and Verify x == y
$cert_A$	$ID_A \mid PK_A \mid sig_{CA}(ID_A \mid PK_A)$

Strong Authentication

Protocol #6

r_1 , $cert_B$

r_2 , $cert_A$, $sig_A(ID_B \mid r_1 \mid r_2)$

$sig_B(ID_A \mid r_2)$

Strong Authentication

Protocol #7

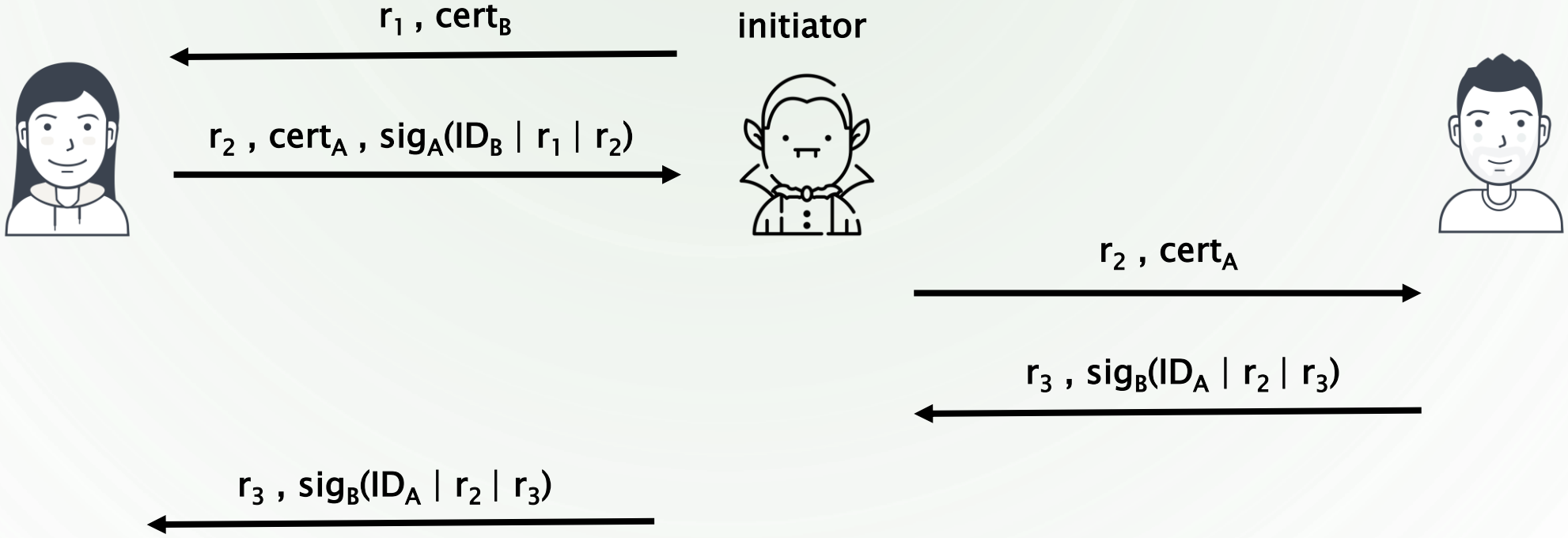
r_1 , $cert_B$

r_2 , $cert_A$, $sig_A(ID_B \mid r_1 \mid r_2)$

r_3 , $sig_B(ID_A \mid r_2 \mid r_3)$

Strong Authentication

Parallel Session Attack



Ref

1. Cryptography Protocols Course, Dr. Hamid Mala, University of Isfahan
2. https://datatracker.ietf.org/doc/html/rfc8235
3. https://blog.goodaudience.com/understanding-zero-knowledge-proofs-through-simple-examples-df673f796d99
4. https://en.wikipedia.org/wiki/Zero-knowledge_proof#Definition
5. https://www.iconfinder.com/UsersInsights
6. https://www.iconfinder.com/Chanut-is