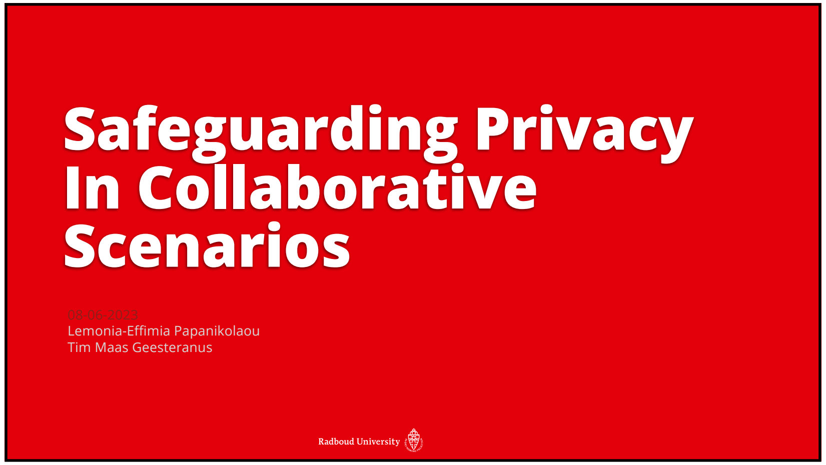


Safeguarding Privacy In Collaborative Scenarios

08-06-2023

Lemonia-Effimia Papanikolaou
Tim Maas Geesteranus

Radboud University

1

PICTURE THIS SCENARIO

Radboud University

2

YES!

Radboud University

3

YES!

Radboud University

4

BUT

Radboud University

5

OR WHAT IF...

Radboud University

6

OR WHAT IF...

Radboud University

7

OR WHAT IF...

Radboud University

8

OR WHAT IF...

Radboud University

9

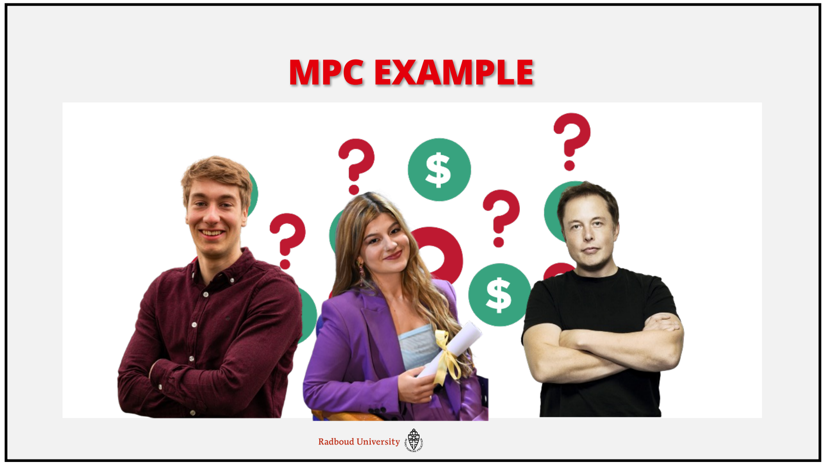
Secure Multiparty Computation

08-06-2023

Lemonia-Effimia Papanikolaou
Tim Maas Geesteranus

Radboud University

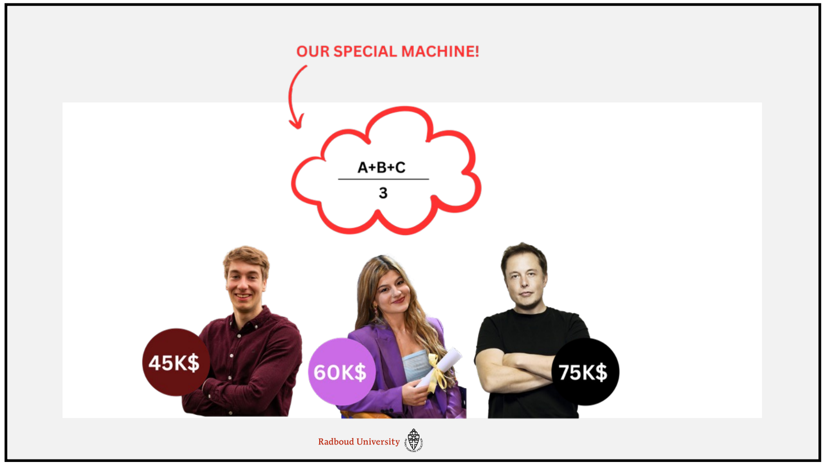
10



MPC EXAMPLE

Radboud University

11

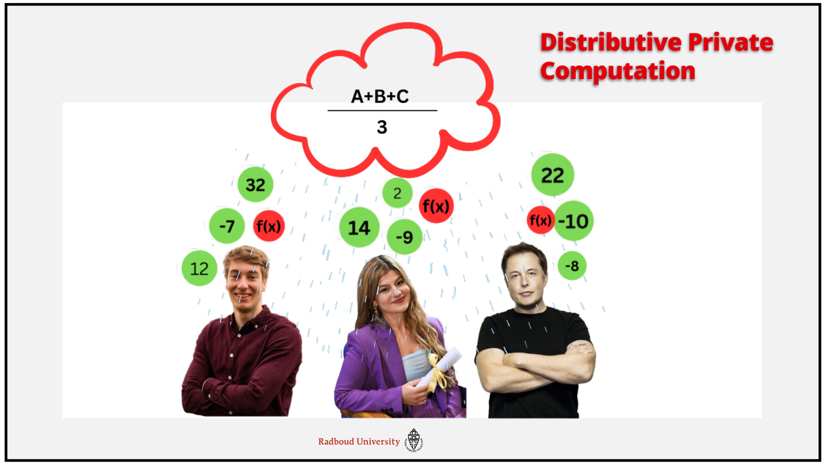


OUR SPECIAL MACHINE!

$$\frac{A+B+C}{3}$$

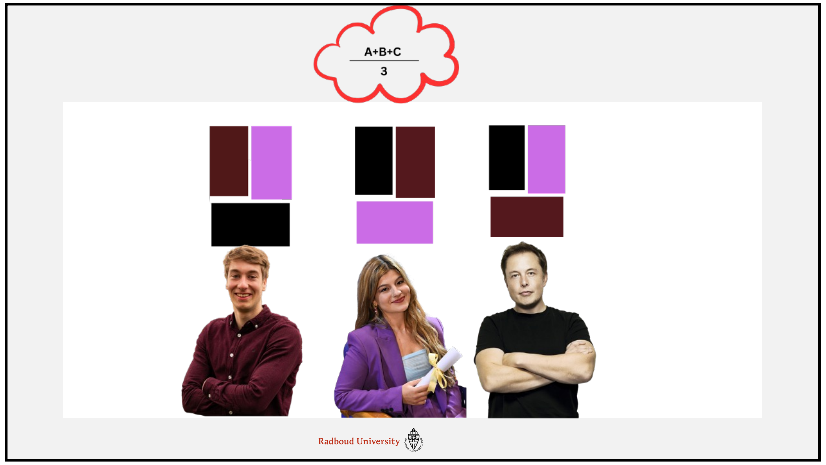
Radboud University

12

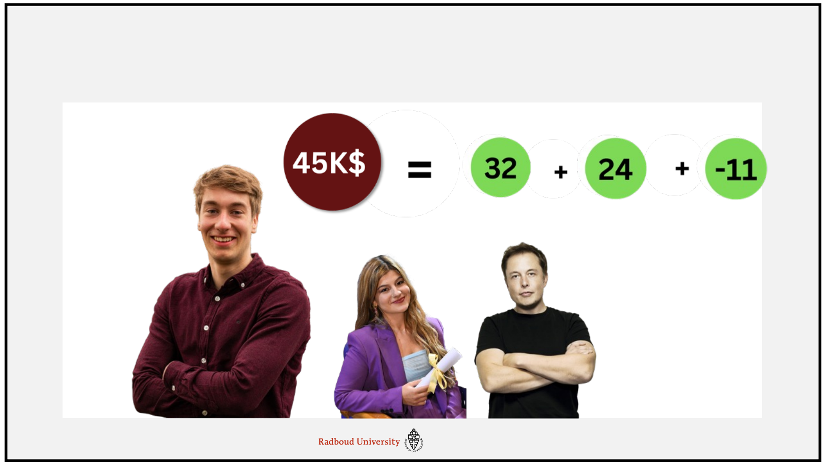


Distributive Private Computation

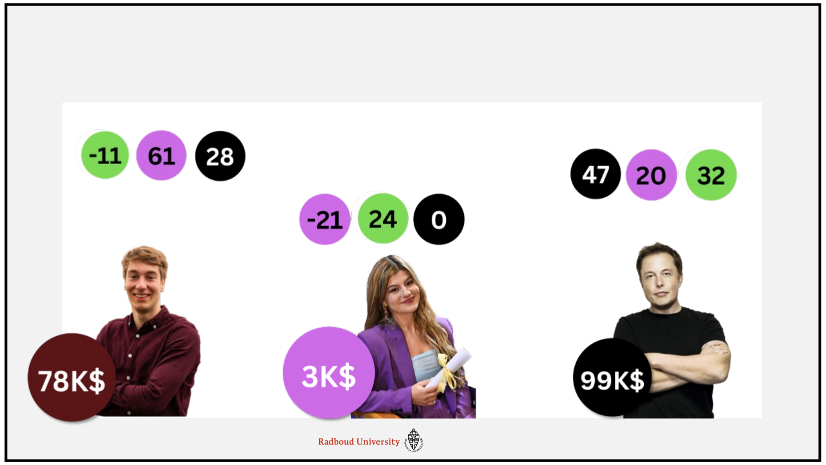
13



14

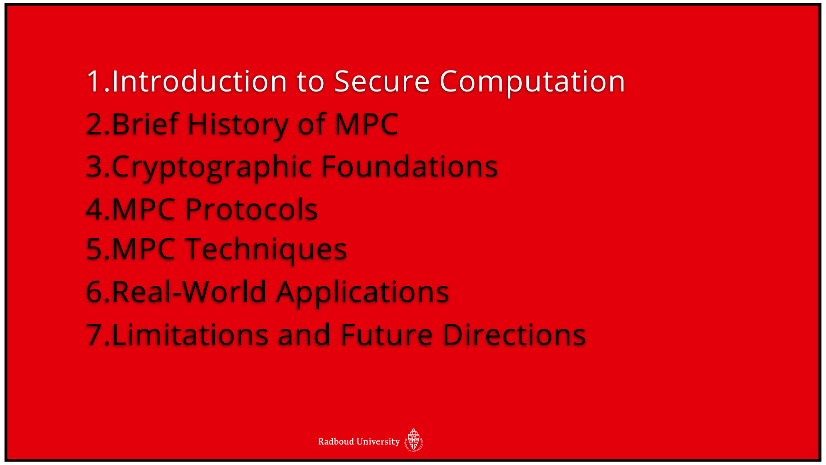


15



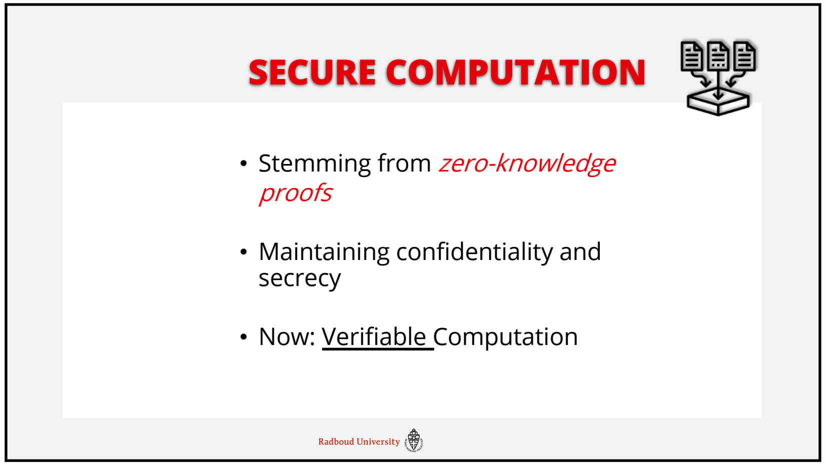
16

17



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

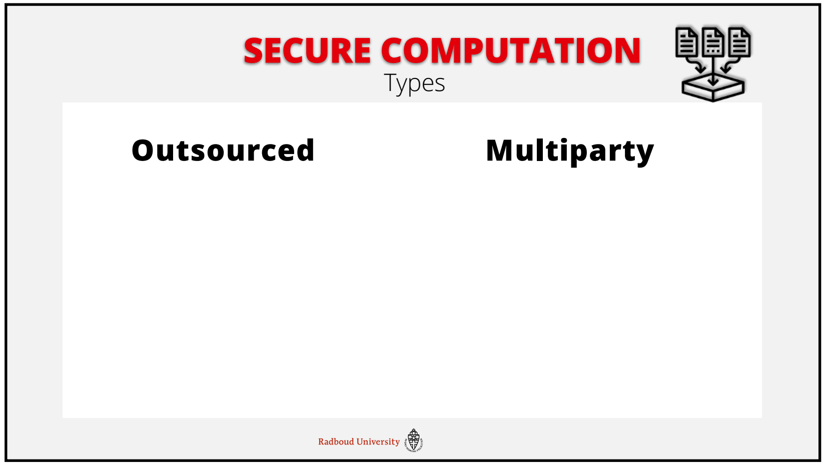
18



SECURE COMPUTATION

- Stemming from *zero-knowledge proofs*
- Maintaining confidentiality and secrecy
- Now: Verifiable Computation

19

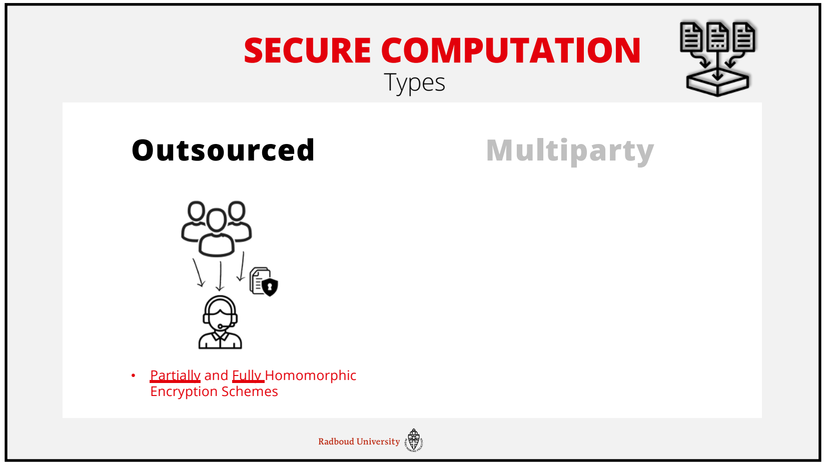


SECURE COMPUTATION

Types

Outsourced **Multiparty**

20



SECURE COMPUTATION
Types

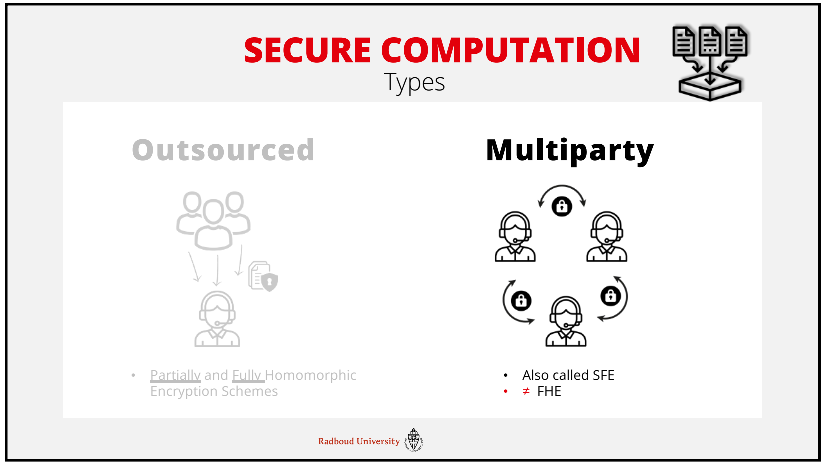
Outsourced

Multiparty

- Partially and Fully Homomorphic Encryption Schemes

Radboud University

21



SECURE COMPUTATION
Types

Outsourced

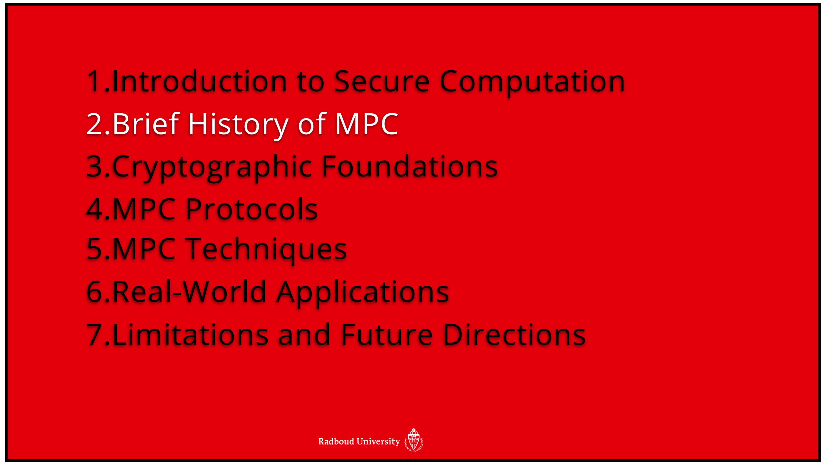
Multiparty

- Partially and Fully Homomorphic Encryption Schemes

- Also called SFE
- ≠ FHE

Radboud University

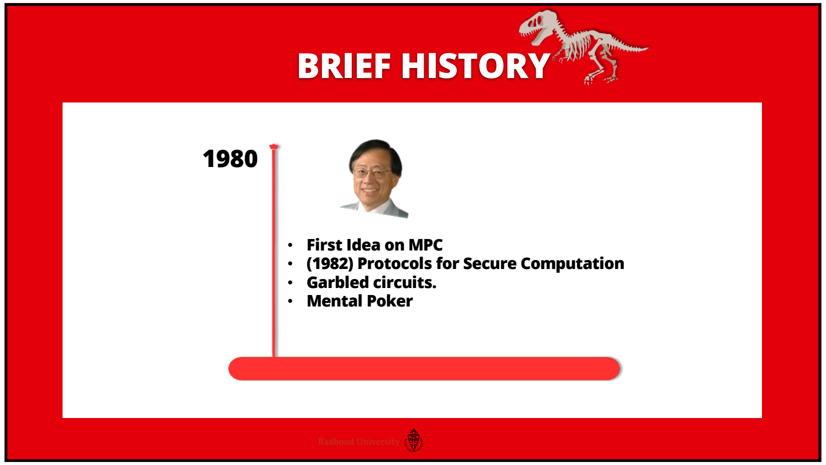
22



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

Radboud University

23



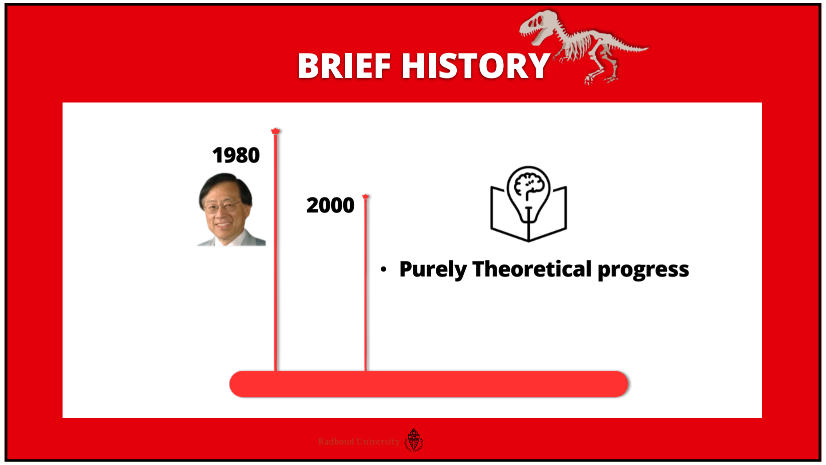
BRIEF HISTORY

1980

- **First Idea on MPC**
- **(1982) Protocols for Secure Computation**
- **Garbled circuits.**
- **Mental Poker**

Radboud University

24

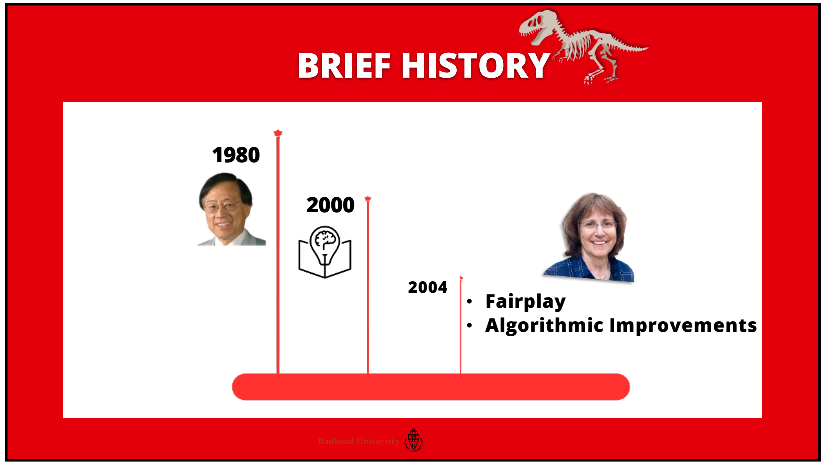


BRIEF HISTORY

- Purely Theoretical progress

Radboud University

25

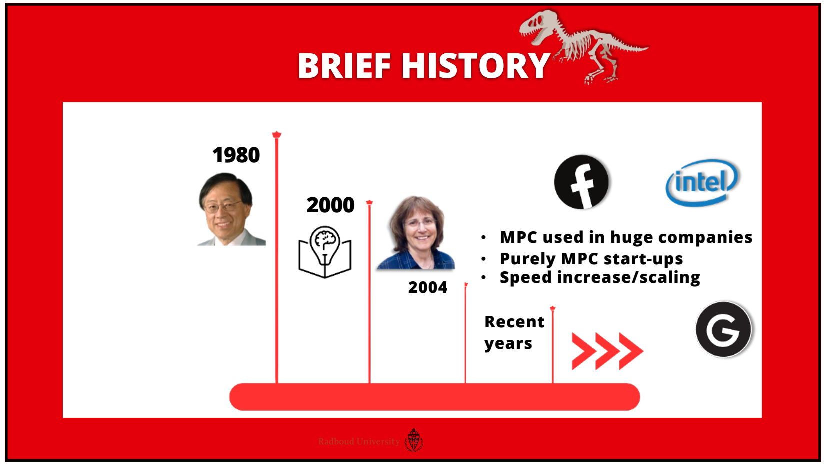


BRIEF HISTORY

- Fairplay
- Algorithmic Improvements

Radboud University

26

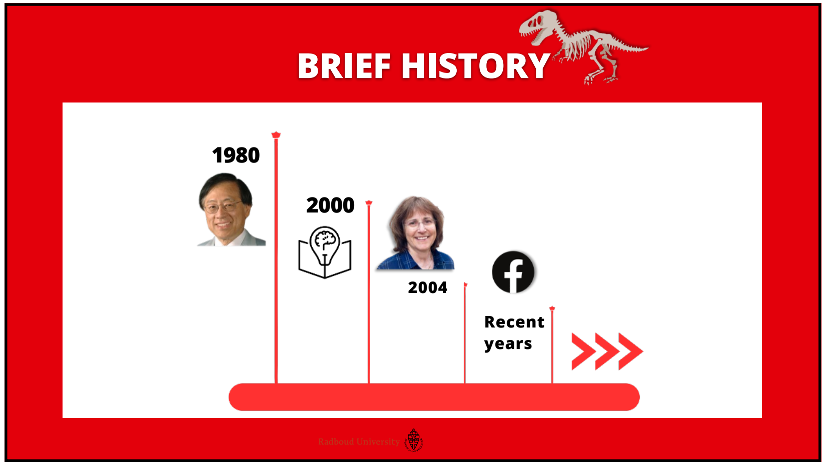


BRIEF HISTORY

- MPC used in huge companies
- Purely MPC start-ups
- Speed increase/scaling

Radboud University

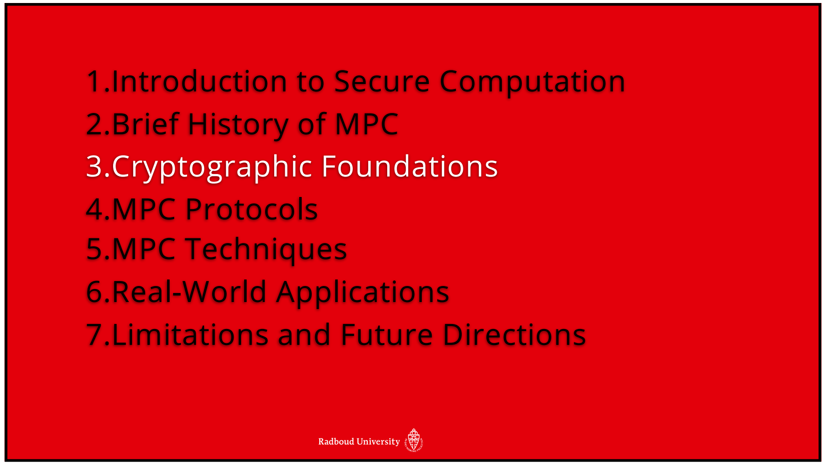
27



BRIEF HISTORY

Radboud University

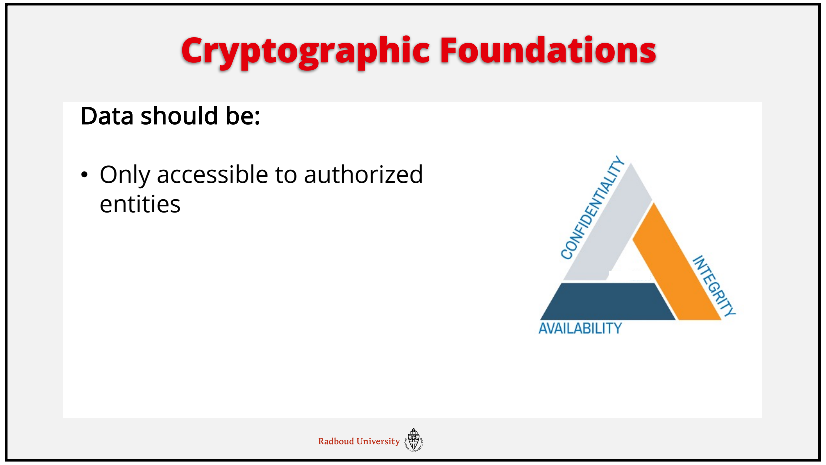
28



1.Introduction to Secure Computation
2.Brief History of MPC
3.Cryptographic Foundations
4.MPC Protocols
5.MPC Techniques
6.Real-World Applications
7.Limitations and Future Directions

Radboud University

29



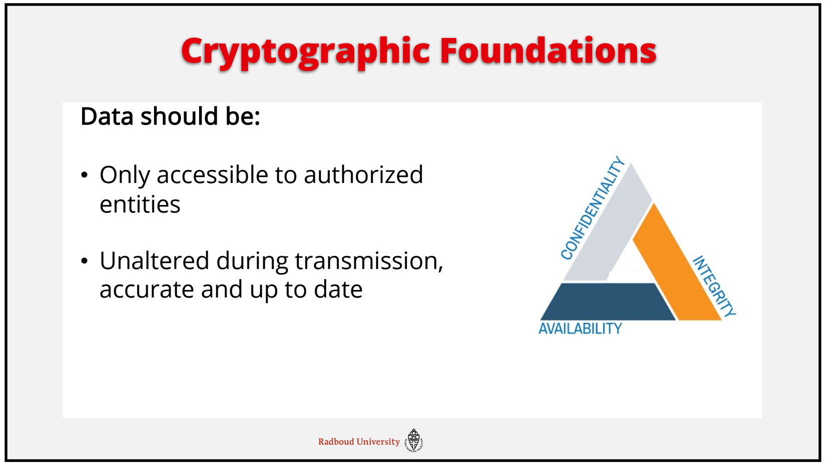
Cryptographic Foundations

Data should be:

- Only accessible to authorized entities

Radboud University

30



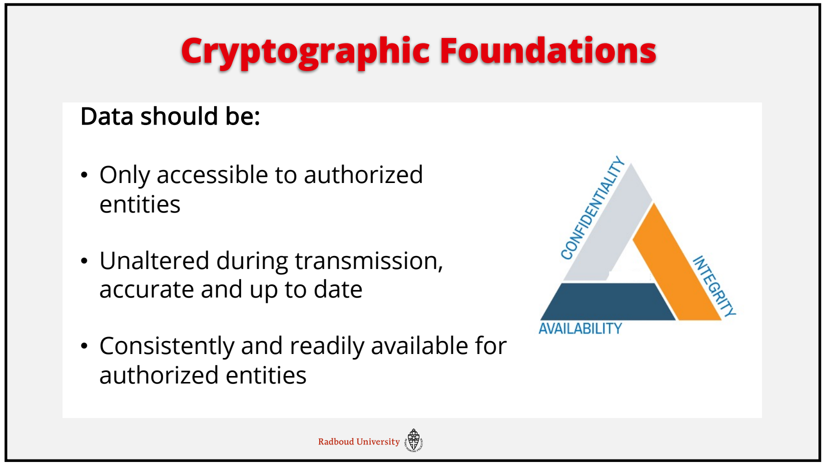
Cryptographic Foundations

Data should be:

- Only accessible to authorized entities
- Unaltered during transmission, accurate and up to date

Radboud University

31



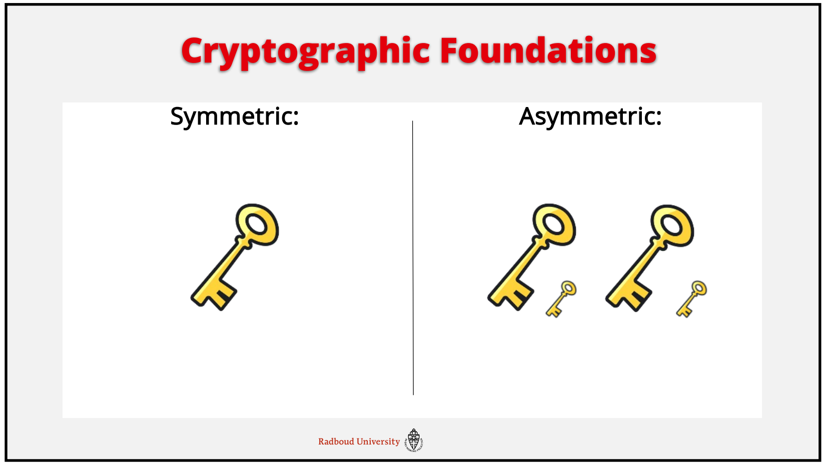
Cryptographic Foundations

Data should be:

- Only accessible to authorized entities
- Unaltered during transmission, accurate and up to date
- Consistently and readily available for authorized entities

Radboud University

32



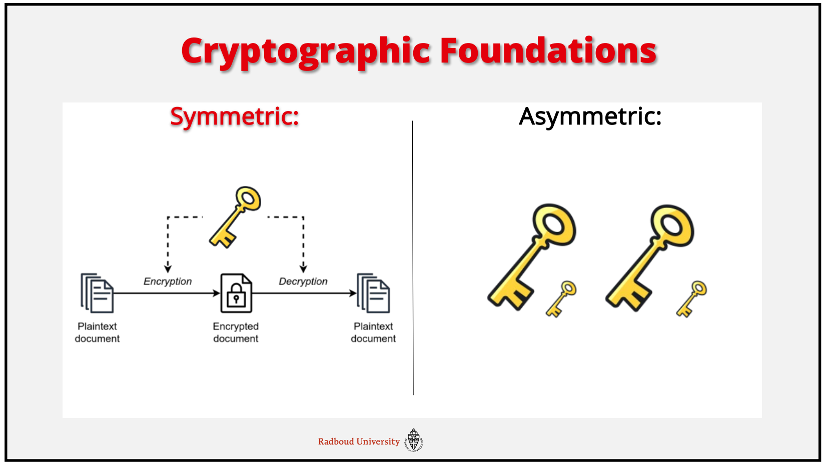
Cryptographic Foundations

Symmetric:

Asymmetric:

Radboud University

33



Cryptographic Foundations

Symmetric:

Encryption

Decryption

Plaintext document

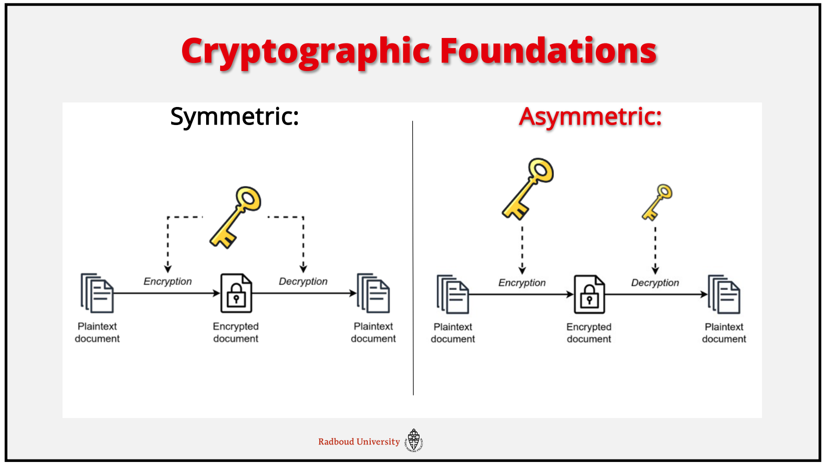
Encrypted document

Plaintext document

Asymmetric:

Radboud University

34



Cryptographic Foundations

Symmetric:

Encryption

Decryption

Plaintext document

Encrypted document

Plaintext document

Asymmetric:

Encryption

Decryption

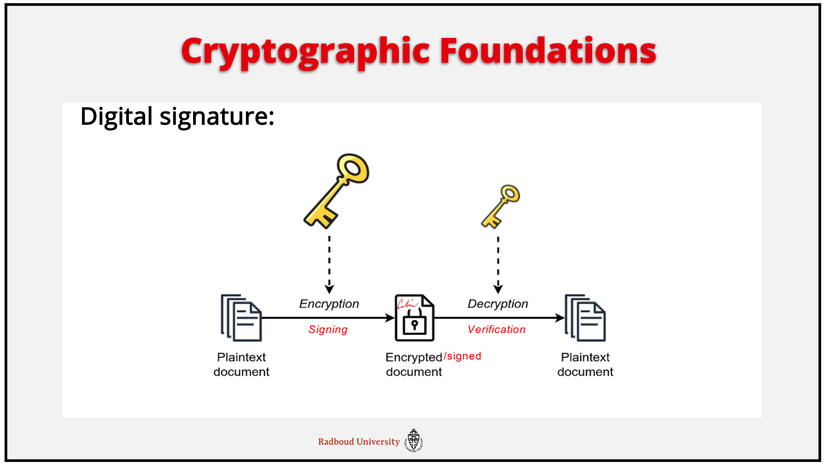
Plaintext document

Encrypted document

Plaintext document

Radboud University

35



Cryptographic Foundations

Digital signature:

Encryption

Signing

Decryption

Verification

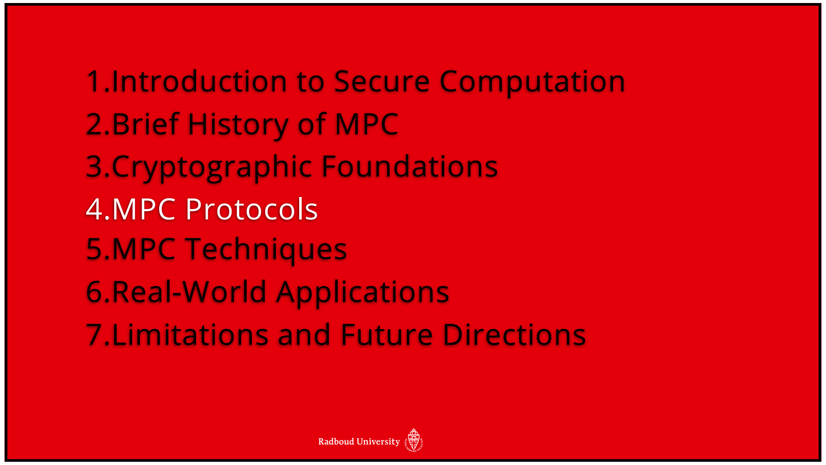
Plaintext document

Encrypted/signed document

Plaintext document

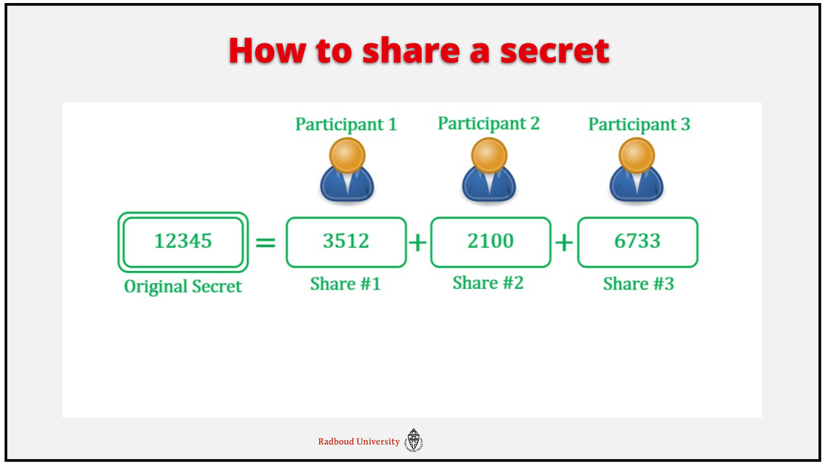
Radboud University

36



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

37



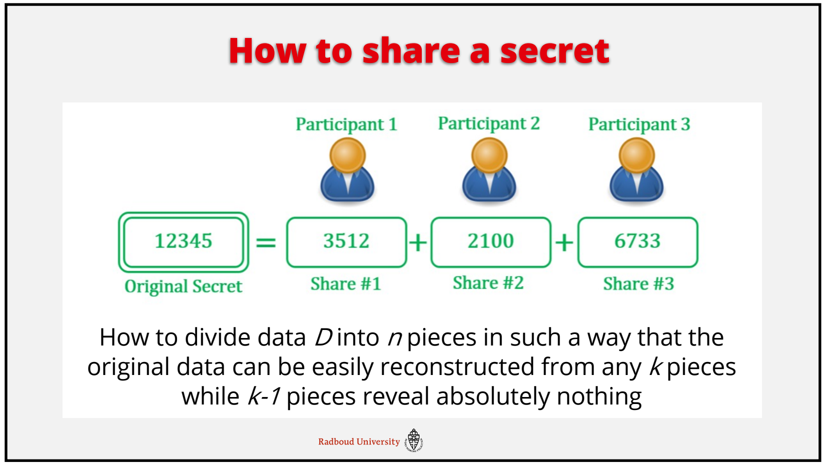
How to share a secret

Participant 1 Participant 2 Participant 3

12345 = 3512 + 2100 + 6733

Original Secret Share #1 Share #2 Share #3

38



How to share a secret

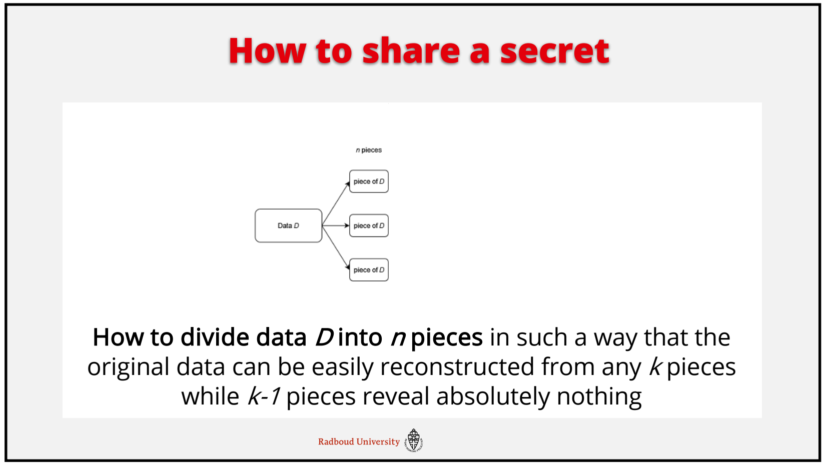
Participant 1 Participant 2 Participant 3

12345 = 3512 + 2100 + 6733

Original Secret Share #1 Share #2 Share #3

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

39



How to share a secret

n pieces

Data *D*

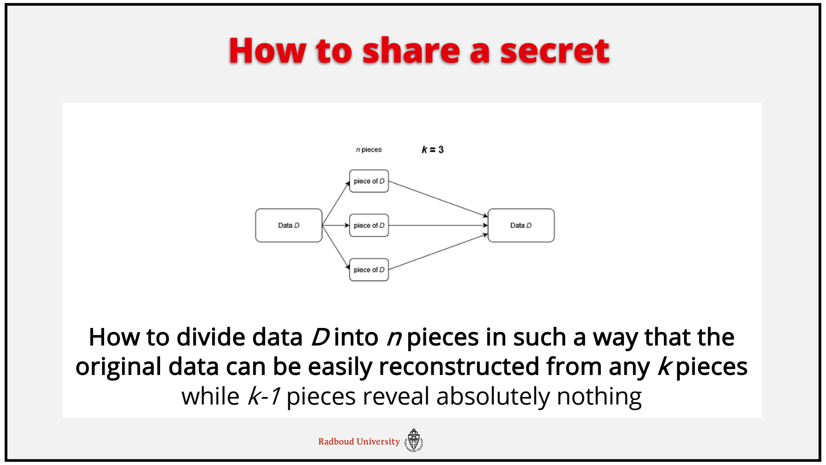
piece of *D*

piece of *D*

piece of *D*

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

40

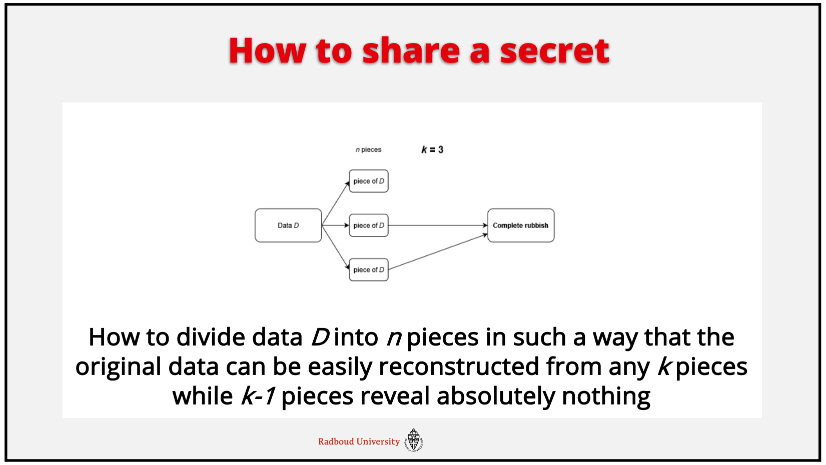


How to share a secret

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

Radboud University

41

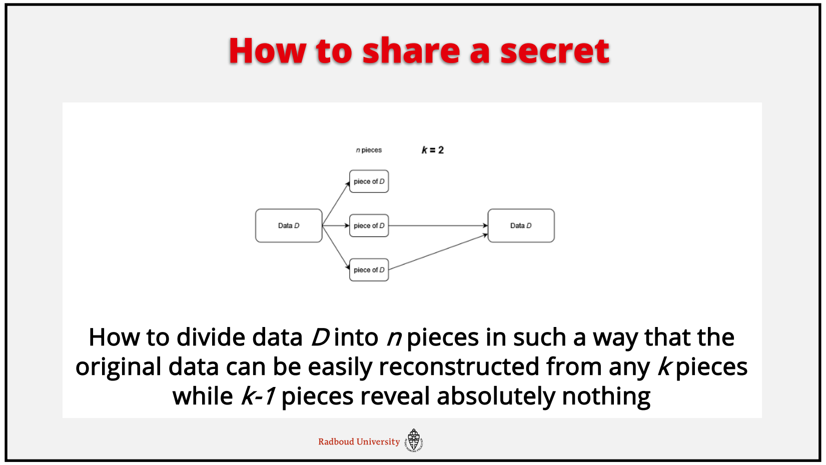


How to share a secret

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

Radboud University

42

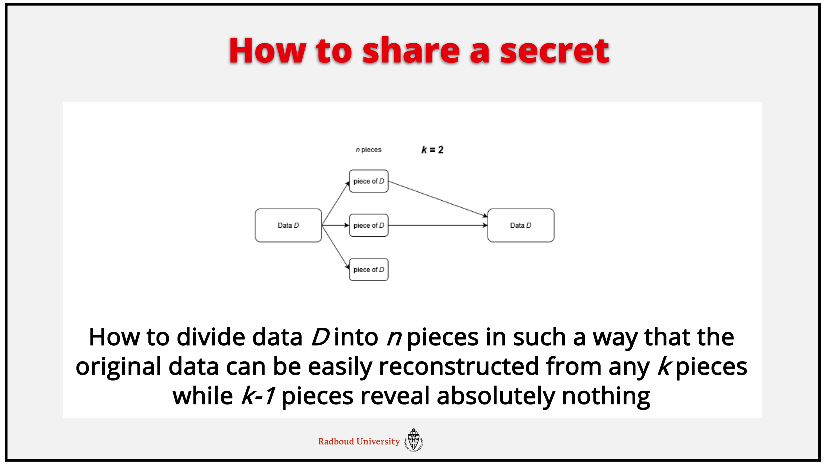


How to share a secret

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

Radboud University

43

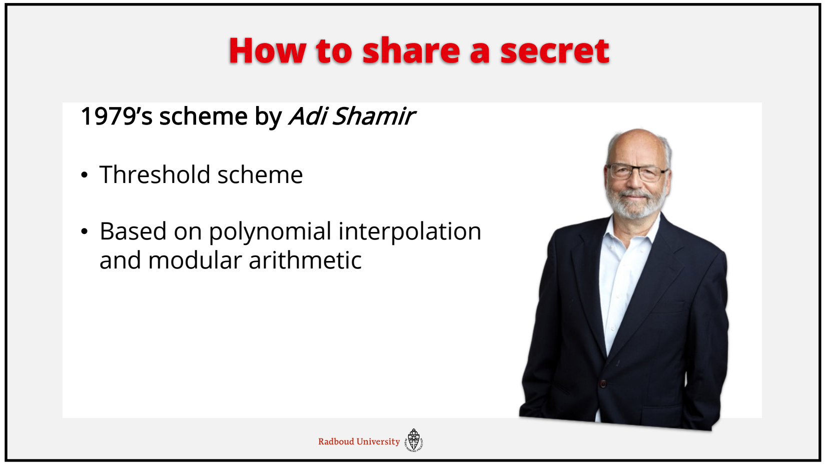


How to share a secret

How to divide data *D* into *n* pieces in such a way that the original data can be easily reconstructed from any *k* pieces while *k-1* pieces reveal absolutely nothing

Radboud University

44



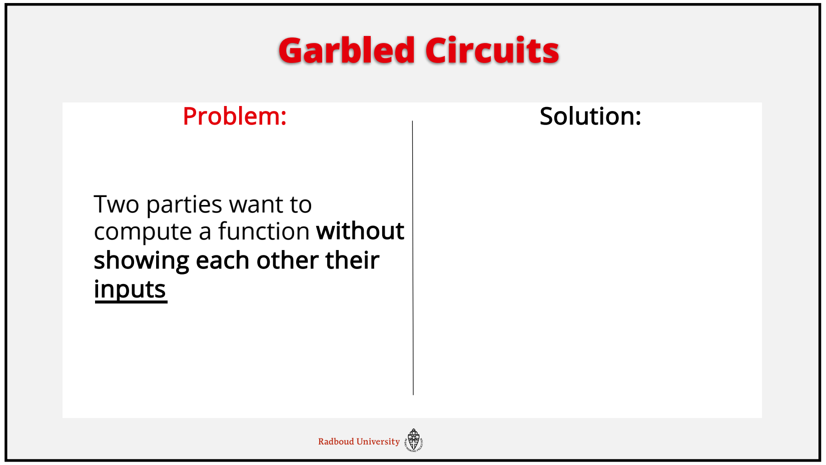
How to share a secret

1979’s scheme by *Adi Shamir*

- Threshold scheme
- Based on polynomial interpolation and modular arithmetic

Radboud University

45



Garbled Circuits

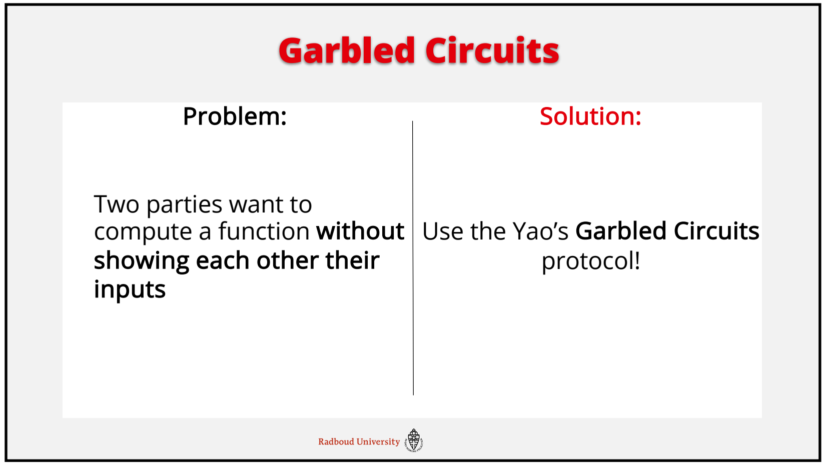
Problem:

Two parties want to compute a function **without showing each other their inputs**

Solution:

Radboud University

46



Garbled Circuits

Problem:

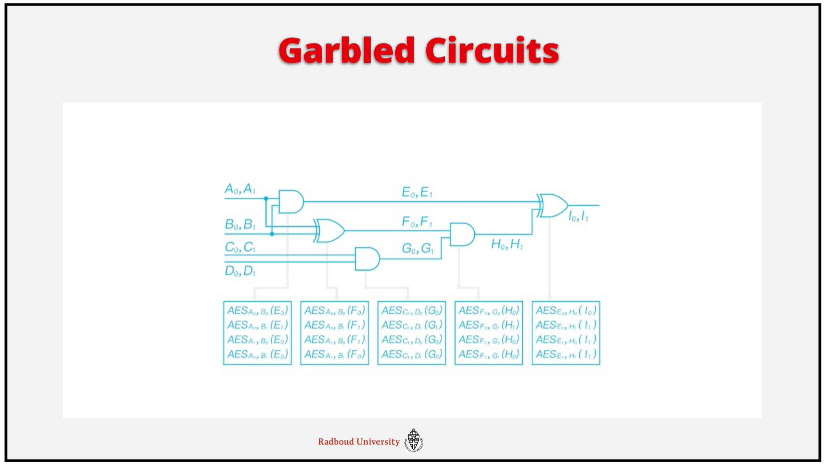
Two parties want to compute a function **without showing each other their inputs**

Solution:

Use the Yao’s **Garbled Circuits** protocol!

Radboud University

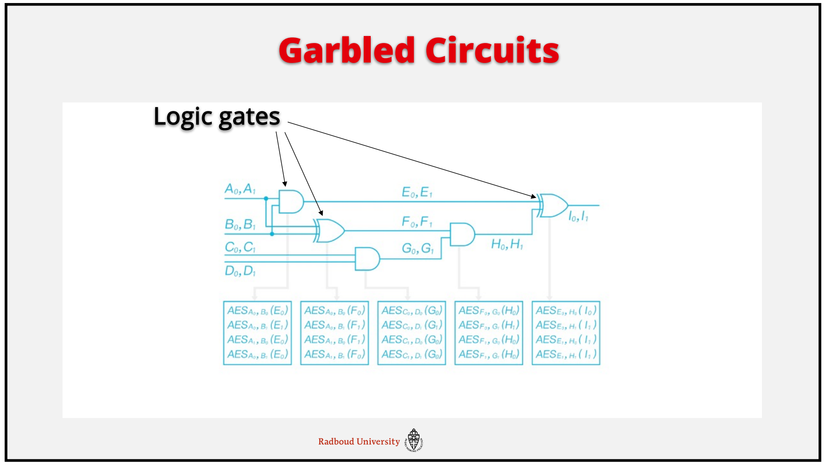
47



Garbled Circuits

Radboud University

48

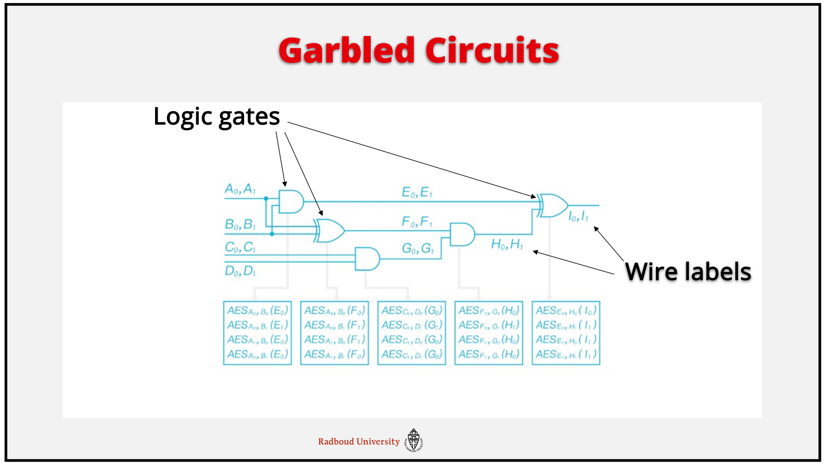


Garbled Circuits

Logic gates

$AES_{A_0, B_0}(E_0)$	$AES_{A_0, B_0}(F_0)$	$AES_{C_0, D_0}(G_0)$	$AES_{F_0, G_0}(H_0)$	$AES_{E_0, H_0}(I_0)$
$AES_{A_0, B_1}(E_1)$	$AES_{A_0, B_1}(F_1)$	$AES_{C_0, D_1}(G_1)$	$AES_{F_0, G_1}(H_1)$	$AES_{E_0, H_1}(I_1)$
$AES_{A_1, B_0}(E_0)$	$AES_{A_1, B_0}(F_1)$	$AES_{C_1, D_0}(G_0)$	$AES_{F_1, G_0}(H_0)$	$AES_{E_1, H_0}(I_1)$
$AES_{A_0, B_1}(E_0)$	$AES_{A_1, B_1}(F_0)$	$AES_{C_1, D_1}(G_0)$	$AES_{F_1, G_1}(H_0)$	$AES_{E_1, H_1}(I_1)$

49



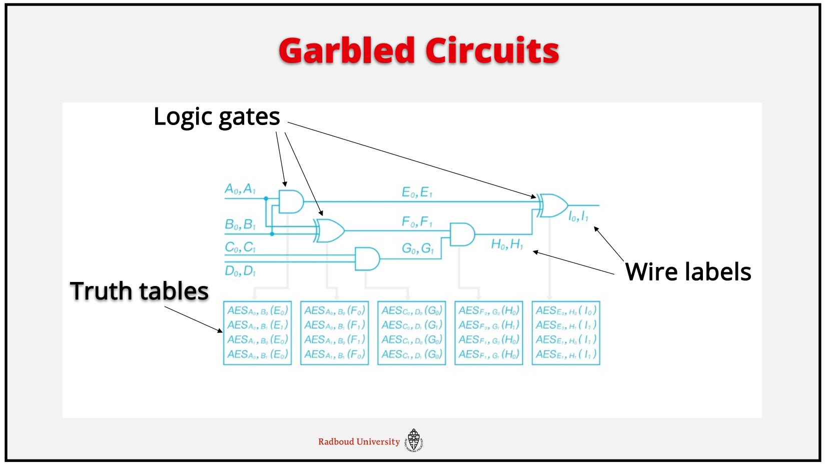
Garbled Circuits

Logic gates

Wire labels

$AES_{A_0, B_0}(E_0)$	$AES_{A_0, B_0}(F_0)$	$AES_{C_0, D_0}(G_0)$	$AES_{F_0, G_0}(H_0)$	$AES_{E_0, H_0}(I_0)$
$AES_{A_0, B_1}(E_1)$	$AES_{A_0, B_1}(F_1)$	$AES_{C_0, D_1}(G_1)$	$AES_{F_0, G_1}(H_1)$	$AES_{E_0, H_1}(I_1)$
$AES_{A_1, B_0}(E_0)$	$AES_{A_1, B_0}(F_1)$	$AES_{C_1, D_0}(G_0)$	$AES_{F_1, G_0}(H_0)$	$AES_{E_1, H_0}(I_1)$
$AES_{A_0, B_1}(E_0)$	$AES_{A_1, B_1}(F_0)$	$AES_{C_1, D_1}(G_0)$	$AES_{F_1, G_1}(H_0)$	$AES_{E_1, H_1}(I_1)$

50



Garbled Circuits

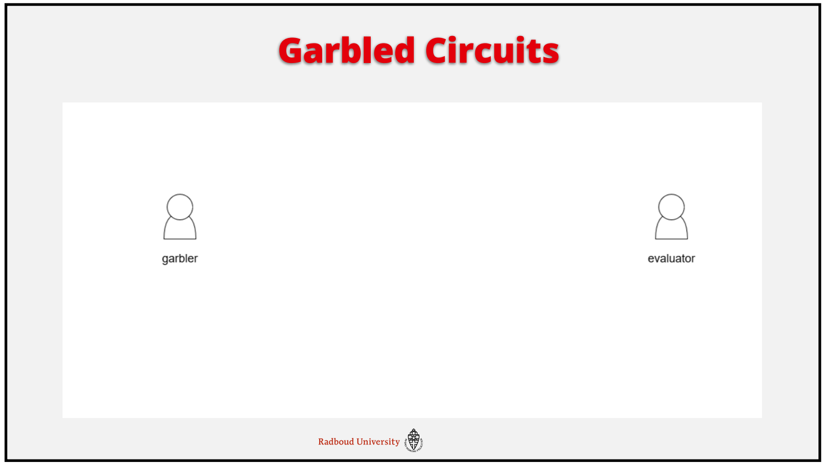
Logic gates

Wire labels

Truth tables

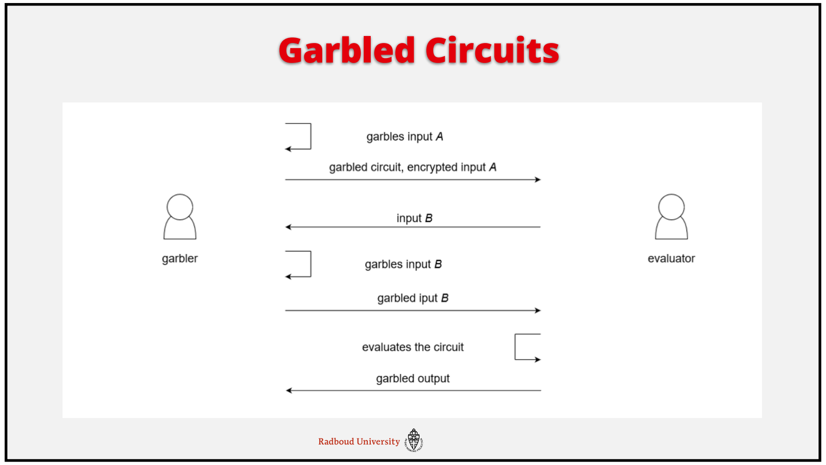
$AES_{A_0, B_0}(E_0)$	$AES_{A_0, B_0}(F_0)$	$AES_{C_0, D_0}(G_0)$	$AES_{F_0, G_0}(H_0)$	$AES_{E_0, H_0}(I_0)$
$AES_{A_0, B_1}(E_1)$	$AES_{A_0, B_1}(F_1)$	$AES_{C_0, D_1}(G_1)$	$AES_{F_0, G_1}(H_1)$	$AES_{E_0, H_1}(I_1)$
$AES_{A_1, B_0}(E_0)$	$AES_{A_1, B_0}(F_1)$	$AES_{C_1, D_0}(G_0)$	$AES_{F_1, G_0}(H_0)$	$AES_{E_1, H_0}(I_1)$
$AES_{A_0, B_1}(E_0)$	$AES_{A_1, B_1}(F_0)$	$AES_{C_1, D_1}(G_0)$	$AES_{F_1, G_1}(H_0)$	$AES_{E_1, H_1}(I_1)$

51



Garbled Circuits

52



Garbled Circuits

garbler

garbles input *A*

garbled circuit, encrypted input *A*

input *B*

garbles input *B*

garbled input *B*

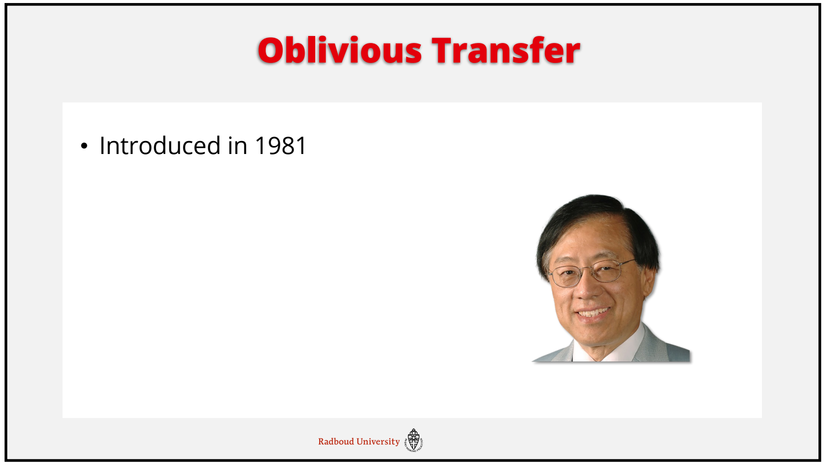
evaluates the circuit

garbled output

evaluator

Radboud University

53

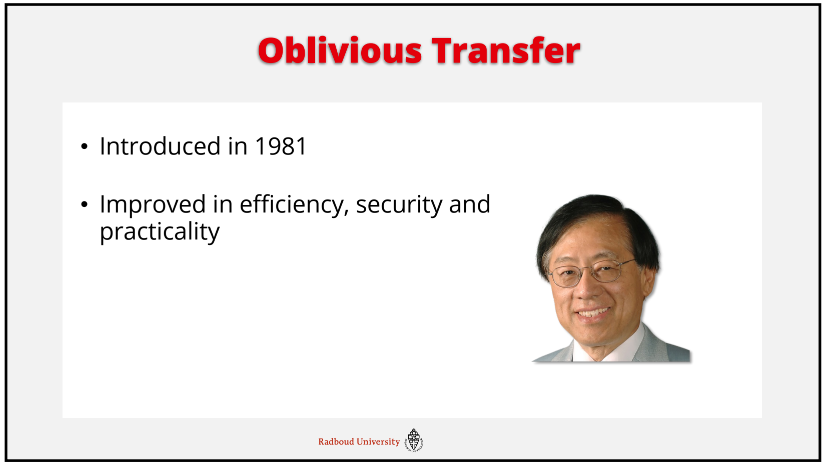


Oblivious Transfer

- Introduced in 1981

Radboud University

54

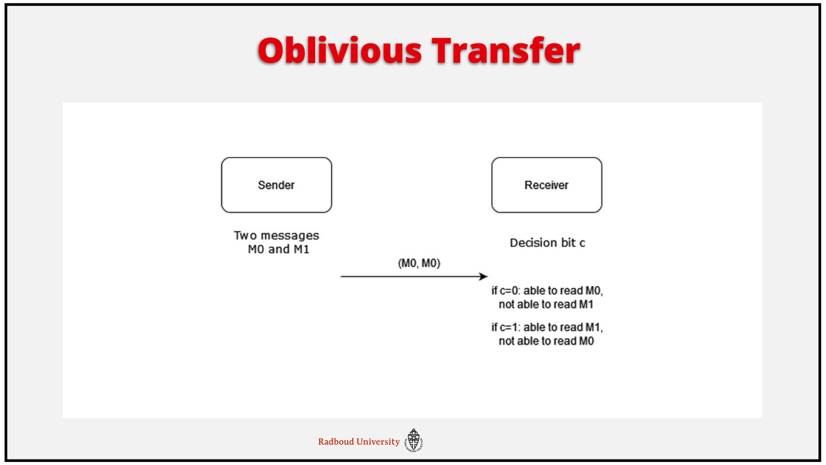


Oblivious Transfer

- Introduced in 1981
- Improved in efficiency, security and practicality

Radboud University

55



Oblivious Transfer

Sender

Two messages
M0 and M1

(M0, M0)

Receiver

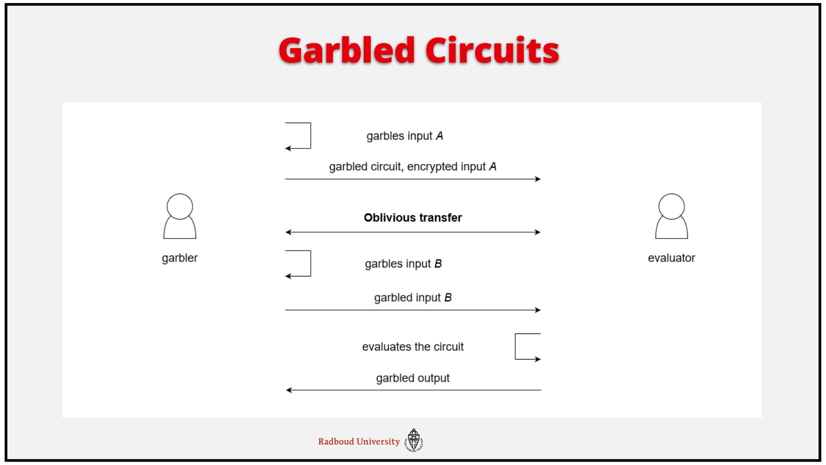
Decision bit c

if c=0: able to read M0,
not able to read M1

if c=1: able to read M1,
not able to read M0

Radboud University

56



Garbled Circuits

garbler

evaluator

garbles input *A*

garbled circuit, encrypted input *A*

Oblivious transfer

garbles input *B*

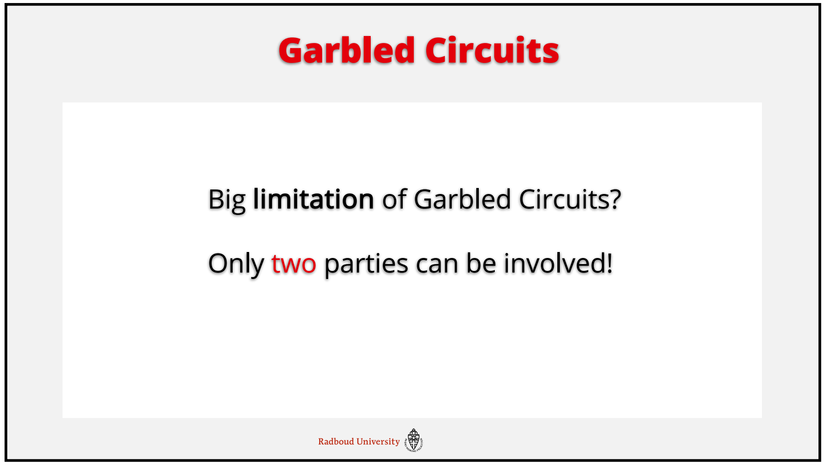
garbled input *B*

evaluates the circuit

garbled output

Radboud University

57



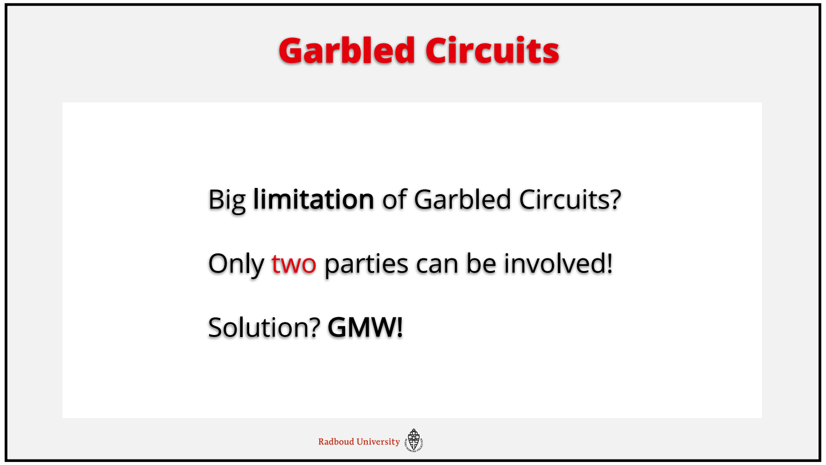
Garbled Circuits

Big **limitation** of Garbled Circuits?

Only two parties can be involved!

Radboud University

58



Garbled Circuits

Big **limitation** of Garbled Circuits?

Only two parties can be involved!

Solution? **GMW!**

Radboud University

59

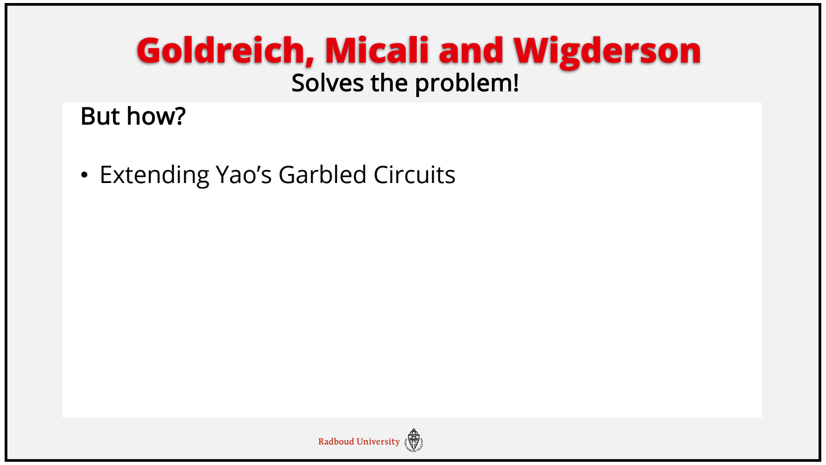
Goldreich, Micali and Wigderson

Solves the problem!

- Developed in 1987
- Designed for multiparty computation

Radboud University

60



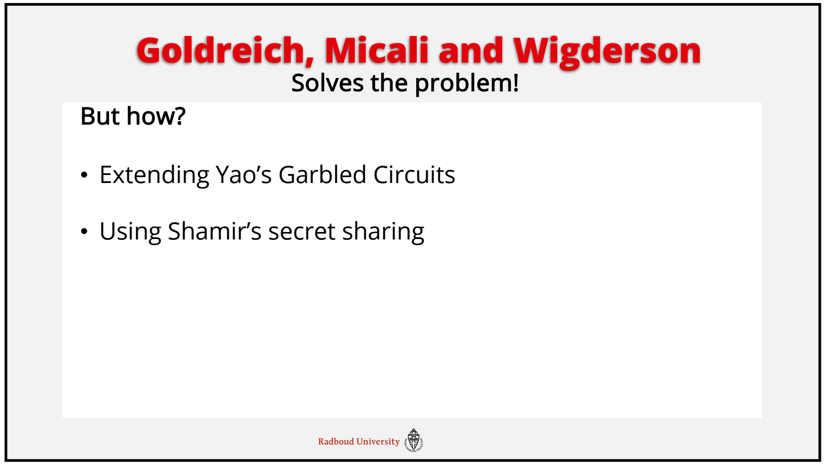
Goldreich, Micali and Wigderson

Solves the problem!

But how?

- Extending Yao's Garbled Circuits

61



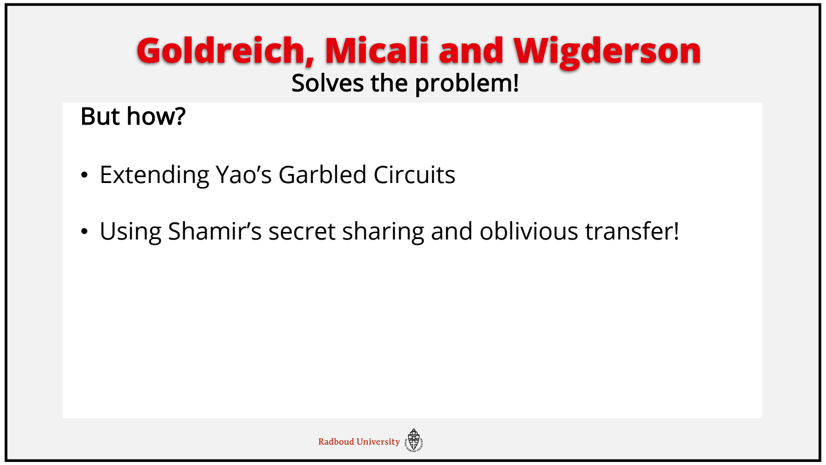
Goldreich, Micali and Wigderson

Solves the problem!

But how?

- Extending Yao's Garbled Circuits
- Using Shamir's secret sharing

62



Goldreich, Micali and Wigderson

Solves the problem!

But how?

- Extending Yao's Garbled Circuits
- Using Shamir's secret sharing and oblivious transfer!

63

Attacks

What do we need to protect?

64

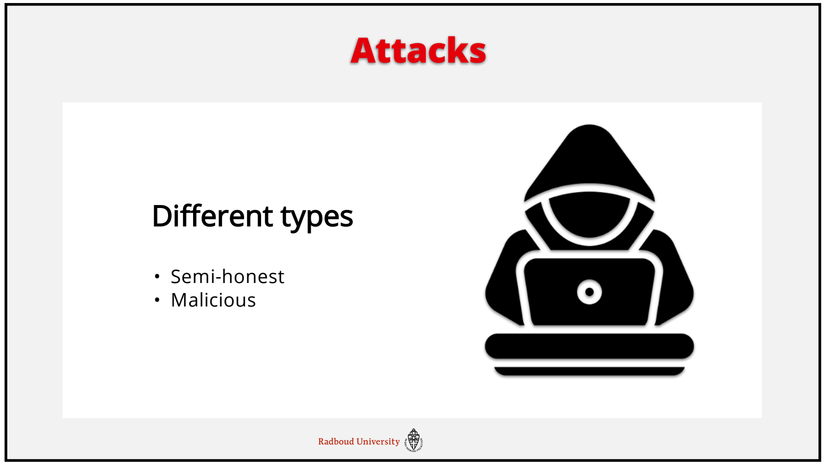
Attacks

What do we need to protect?

- Correctness
- Privacy

Radboud University

65



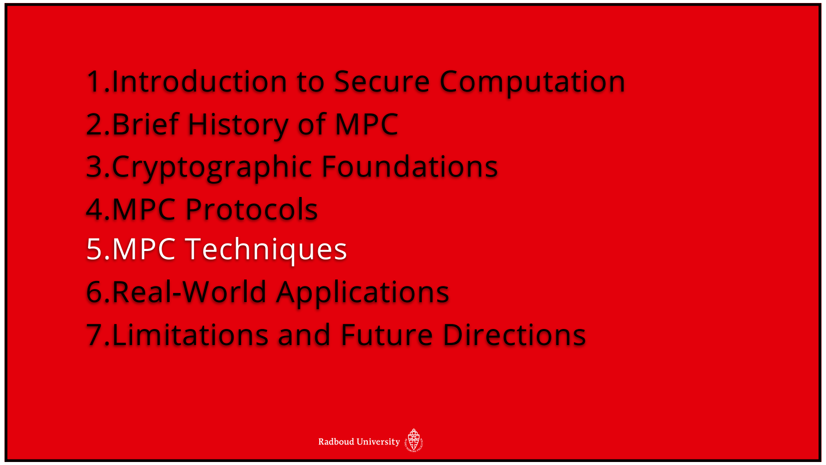
Attacks

Different types

- Semi-honest
- Malicious

Radboud University

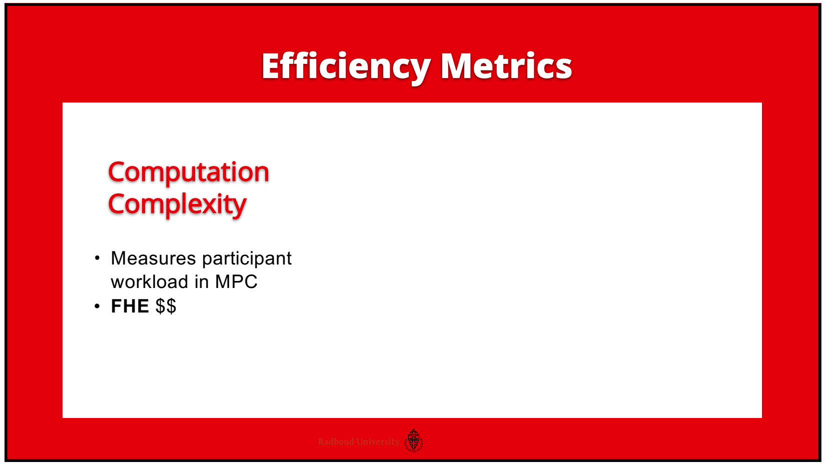
66



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

Radboud University

67



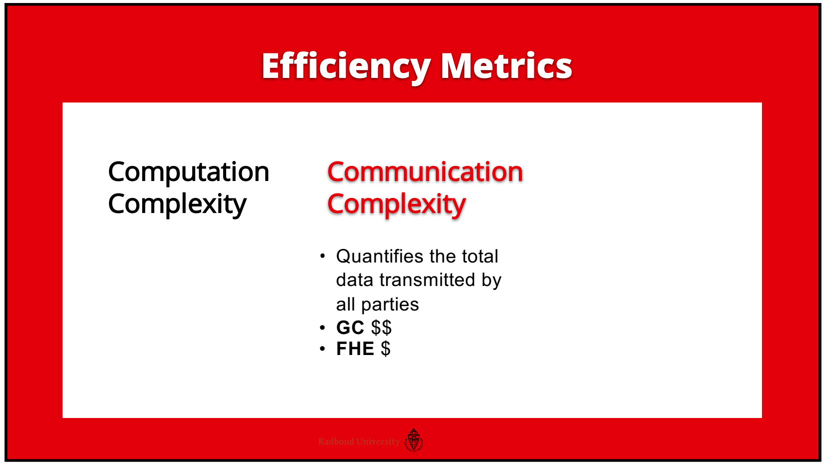
Efficiency Metrics

Computation Complexity

- Measures participant workload in MPC
- **FHE** $$

Radboud University

68



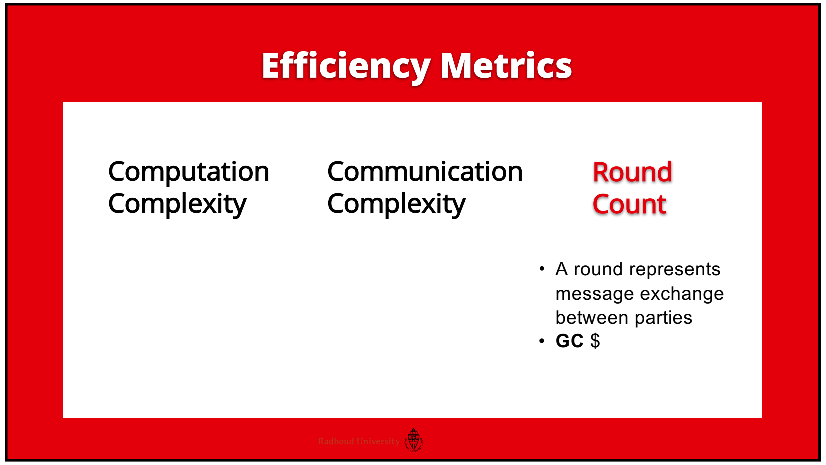
Efficiency Metrics

Computation Complexity

Communication Complexity

- Quantifies the total data transmitted by all parties
- **GC** $$
- **FHE** $

69



Efficiency Metrics

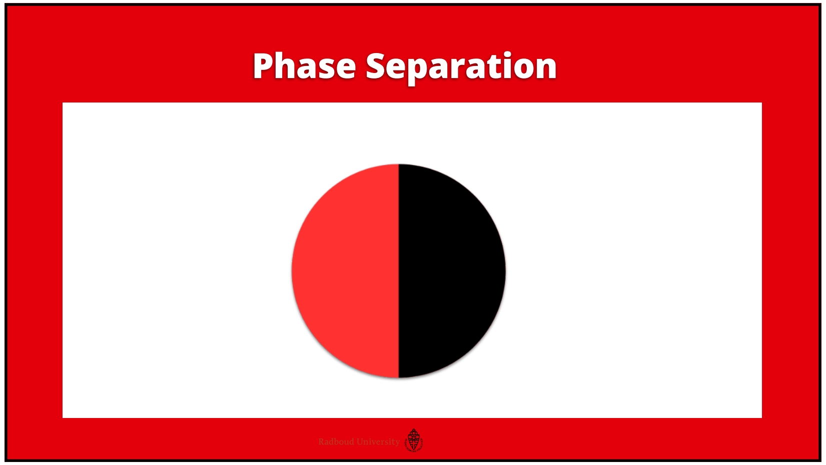
Computation Complexity

Communication Complexity

Round Count

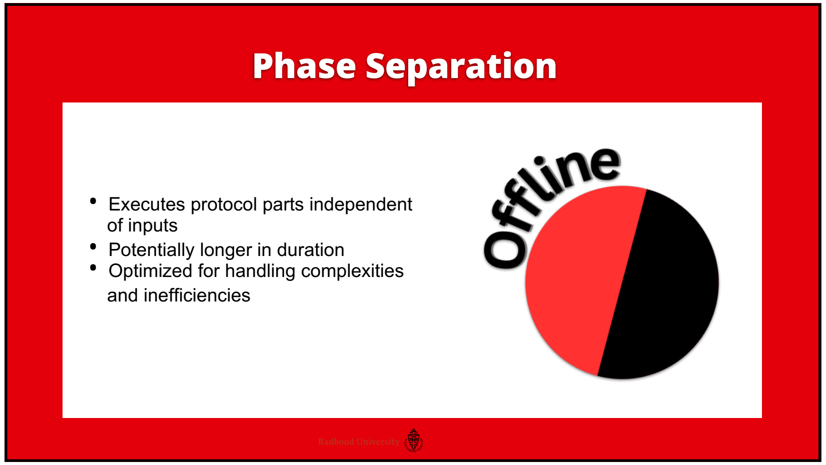
- A round represents message exchange between parties
- **GC** $

70



Phase Separation

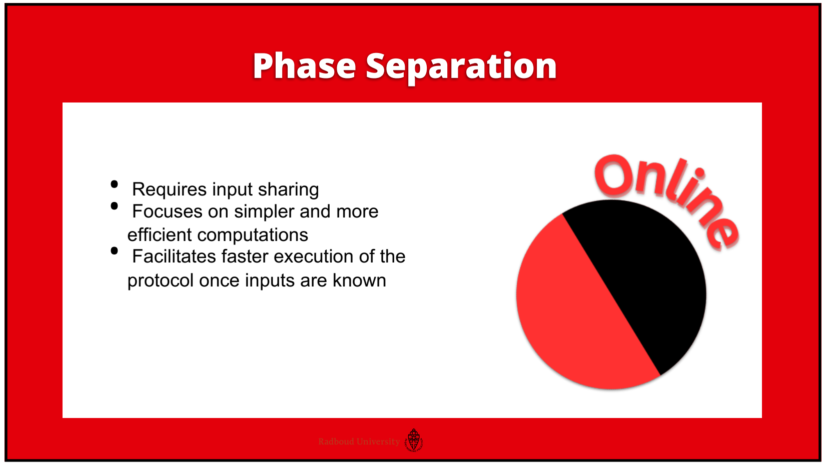
71



Phase Separation

- Executes protocol parts independent of inputs
- Potentially longer in duration
- Optimized for handling complexities and inefficiencies

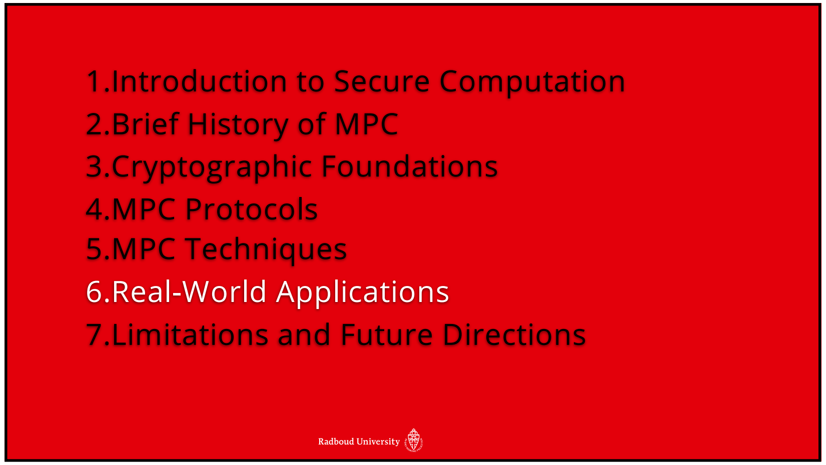
72



Phase Separation

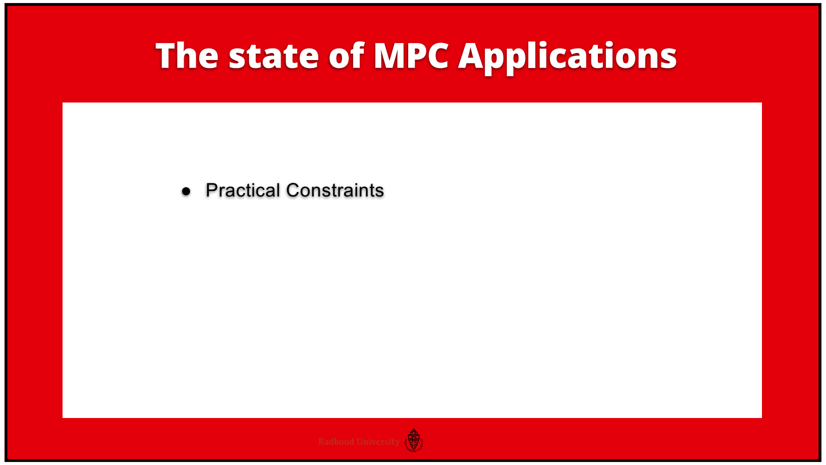
- Requires input sharing
- Focuses on simpler and more efficient computations
- Facilitates faster execution of the protocol once inputs are known

73



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

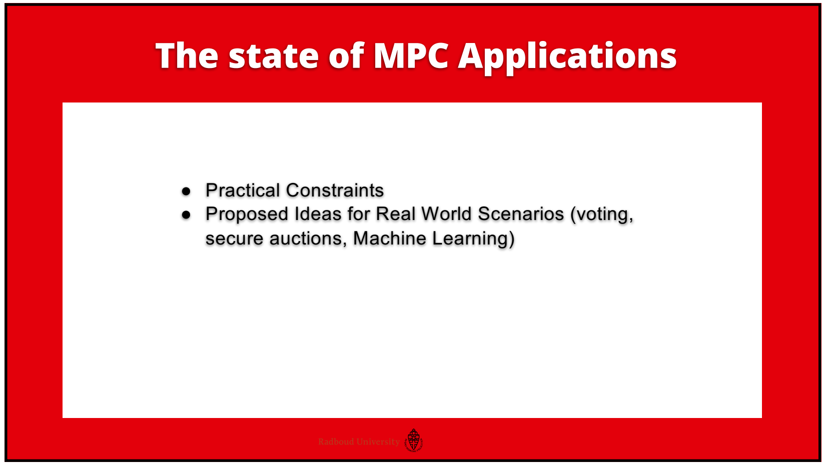
74



The state of MPC Applications

- Practical Constraints

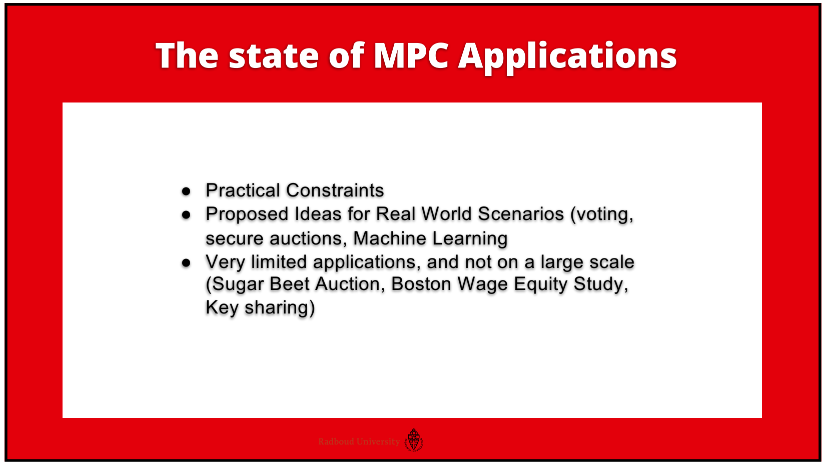
75



The state of MPC Applications

- Practical Constraints
- Proposed Ideas for Real World Scenarios (voting, secure auctions, Machine Learning)

76

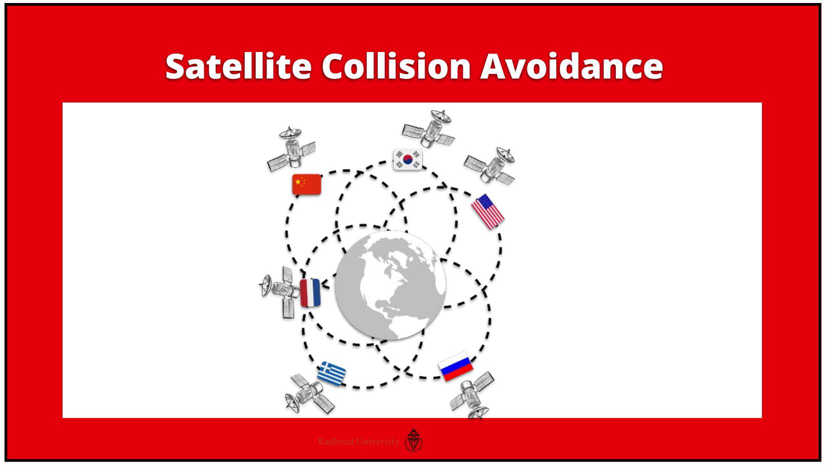


The state of MPC Applications

- Practical Constraints
- Proposed Ideas for Real World Scenarios (voting, secure auctions, Machine Learning
- Very limited applications, and not on a large scale (Sugar Beet Auction, Boston Wage Equity Study, Key sharing)

Radboud University

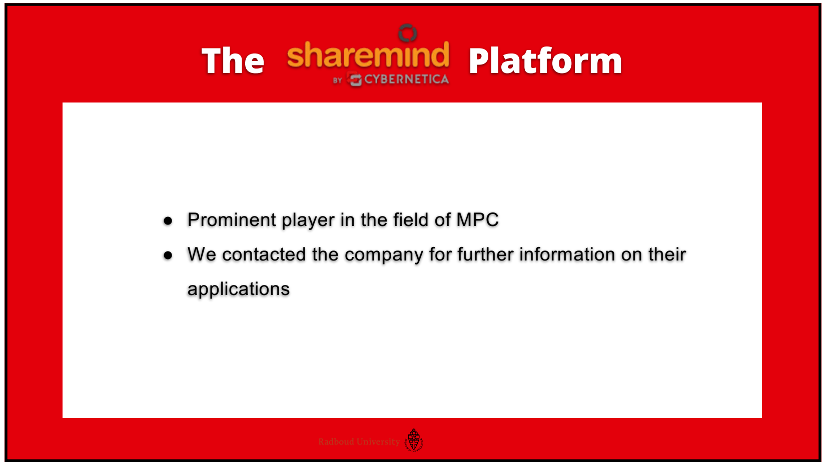
77



Satellite Collision Avoidance

Radboud University

78

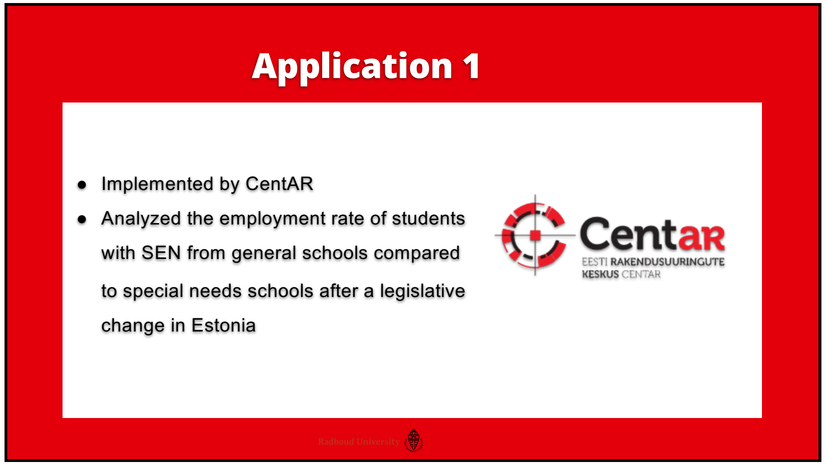


The sharemind BY CYBERNETICA Platform

- Prominent player in the field of MPC
- We contacted the company for further information on their applications

Radboud University

79



Application 1

- Implemented by CentAR
- Analyzed the employment rate of students with SEN from general schools compared to special needs schools after a legislative change in Estonia

Centar EESTI RAKENDUSUURINGUTE KESKUS CENTAR

Radboud University

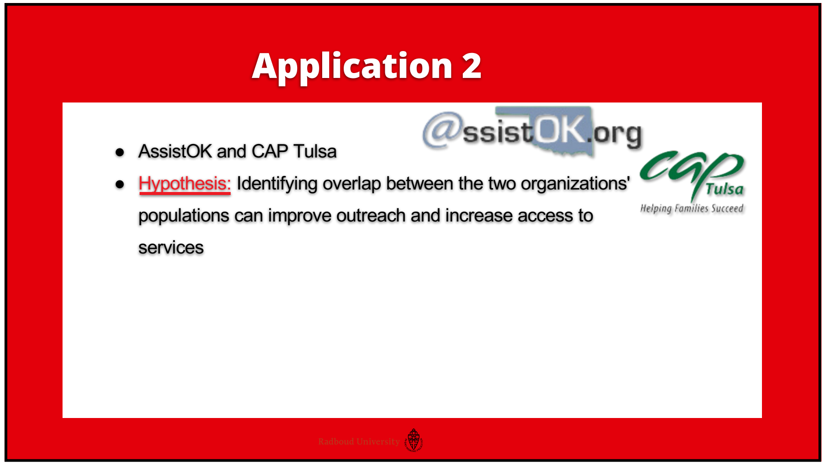
80

Application 2

- AssistOK and CAP Tulsa

@ssistOK.org
cap Tulsa
Helping Families Succeed
Radboud University

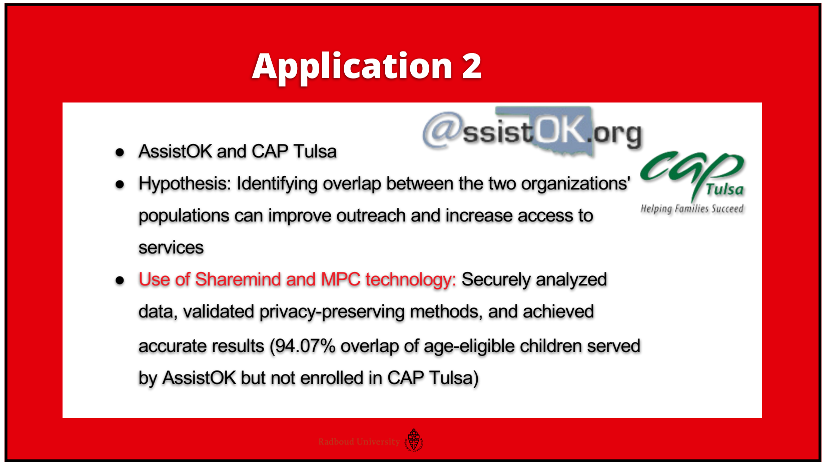
81



Application 2

- AssistOK and CAP Tulsa
- Hypothesis: Identifying overlap between the two organizations' populations can improve outreach and increase access to services

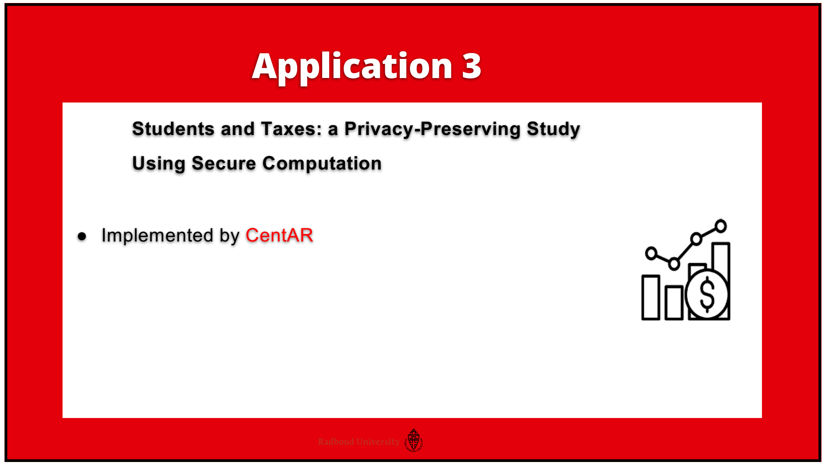
82



Application 2

- AssistOK and CAP Tulsa
- Hypothesis: Identifying overlap between the two organizations' populations can improve outreach and increase access to services
- Use of Sharemind and MPC technology: Securely analyzed data, validated privacy-preserving methods, and achieved accurate results (94.07% overlap of age-eligible children served by AssistOK but not enrolled in CAP Tulsa)

83

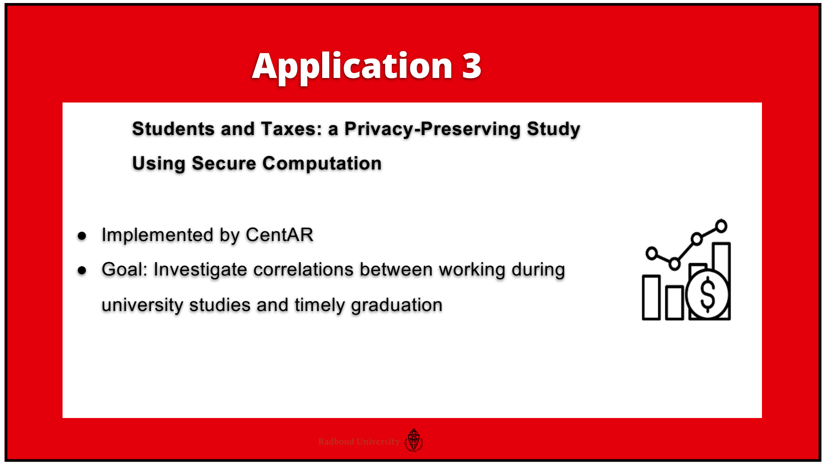


Application 3

Students and Taxes: a Privacy-Preserving Study Using Secure Computation

- Implemented by CentAR

84

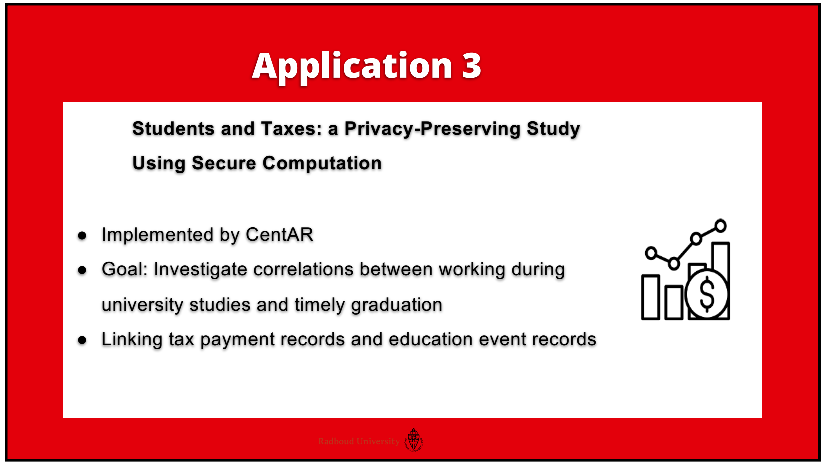


Application 3

Students and Taxes: a Privacy-Preserving Study Using Secure Computation

- Implemented by CentAR
- Goal: Investigate correlations between working during university studies and timely graduation

85

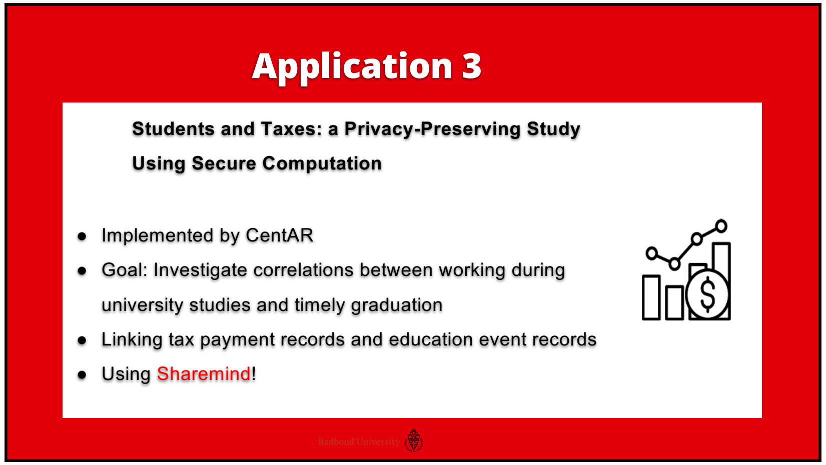


Application 3

Students and Taxes: a Privacy-Preserving Study Using Secure Computation

- Implemented by CentAR
- Goal: Investigate correlations between working during university studies and timely graduation
- Linking tax payment records and education event records

86

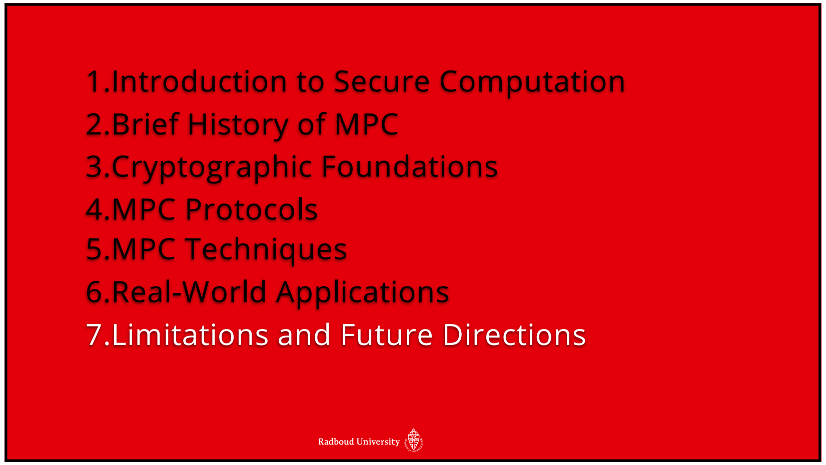


Application 3

Students and Taxes: a Privacy-Preserving Study Using Secure Computation

- Implemented by CentAR
- Goal: Investigate correlations between working during university studies and timely graduation
- Linking tax payment records and education event records
- Using Sharemind!

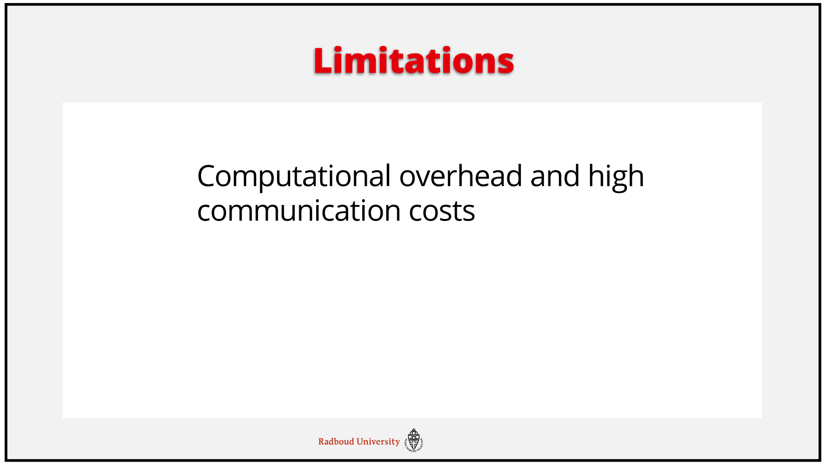
87



1. Introduction to Secure Computation
2. Brief History of MPC
3. Cryptographic Foundations
4. MPC Protocols
5. MPC Techniques
6. Real-World Applications
7. Limitations and Future Directions

Radboud University

88

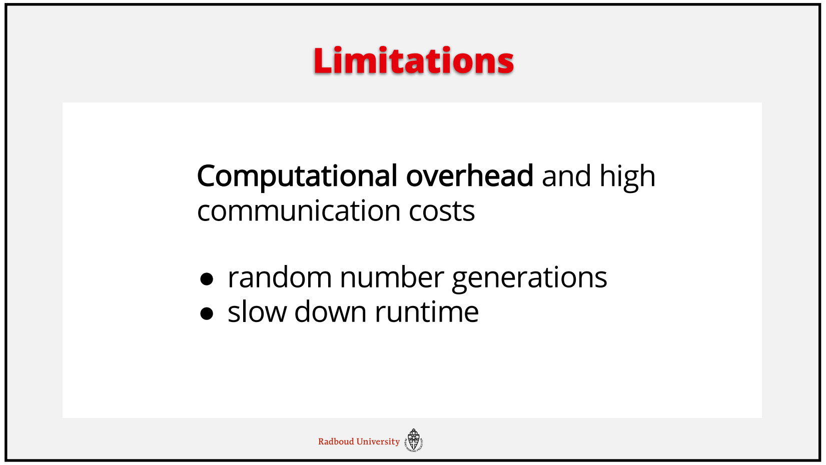


Limitations

Computational overhead and high communication costs

Radboud University

89



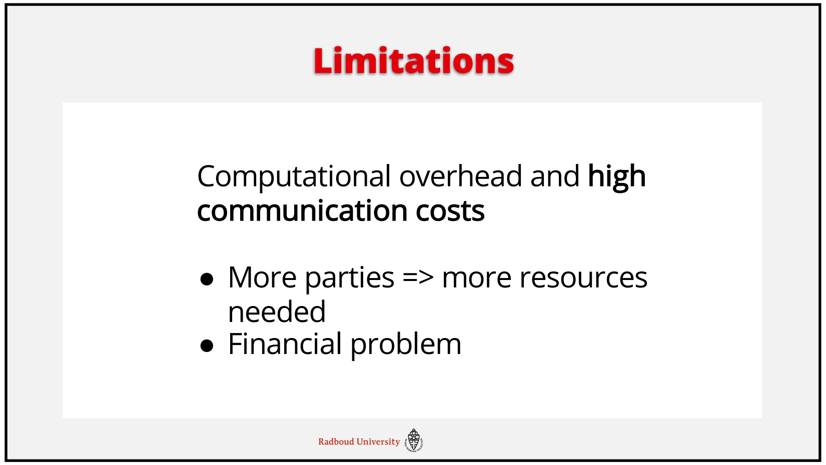
Limitations

Computational overhead and high communication costs

- random number generations
- slow down runtime

Radboud University

90



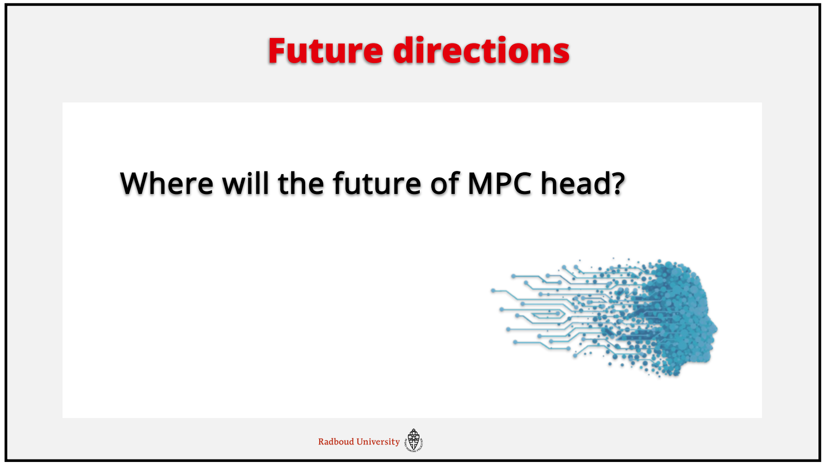
Limitations

Computational overhead and **high communication costs**

- More parties => more resources needed
- Financial problem

Radboud University

91

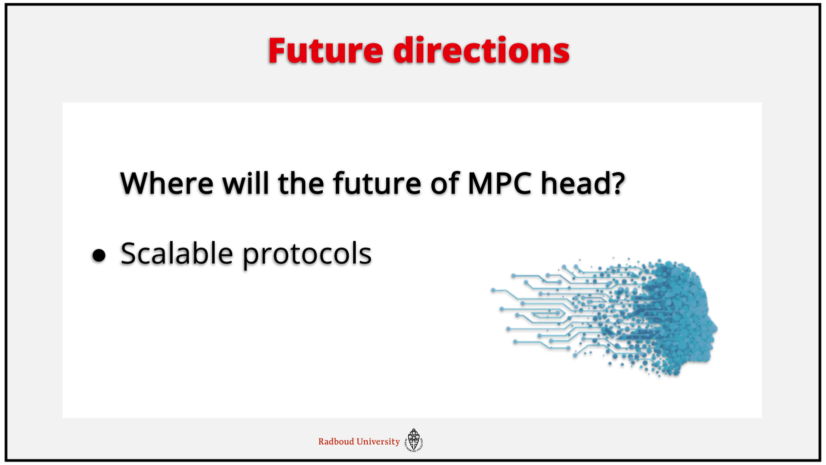


Future directions

Where will the future of MPC head?

Radboud University

92

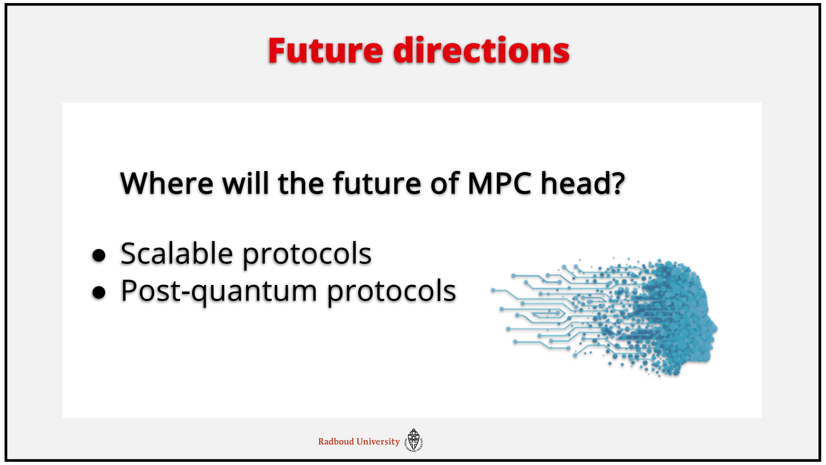


Future directions

Where will the future of MPC head?

- Scalable protocols

93

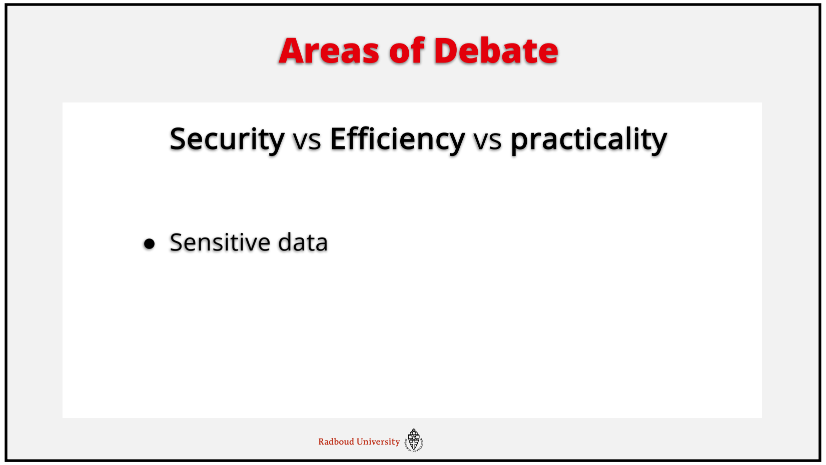


Future directions

Where will the future of MPC head?

- Scalable protocols
- Post-quantum protocols

94

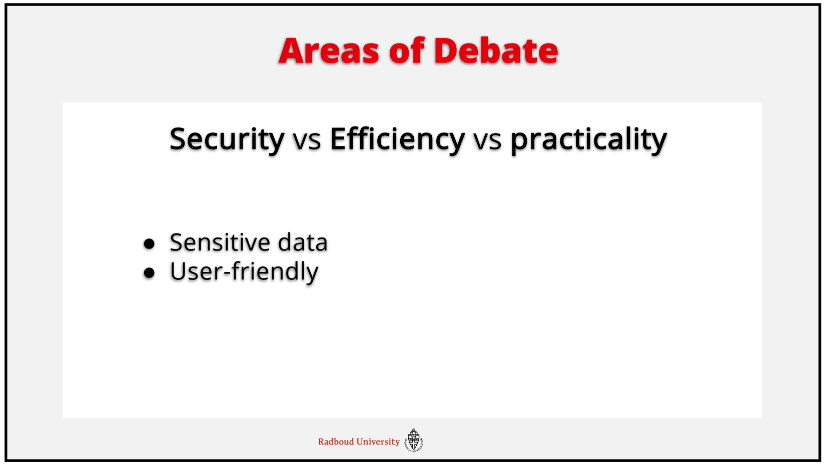


Areas of Debate

Security vs Efficiency vs practicality

- Sensitive data

95

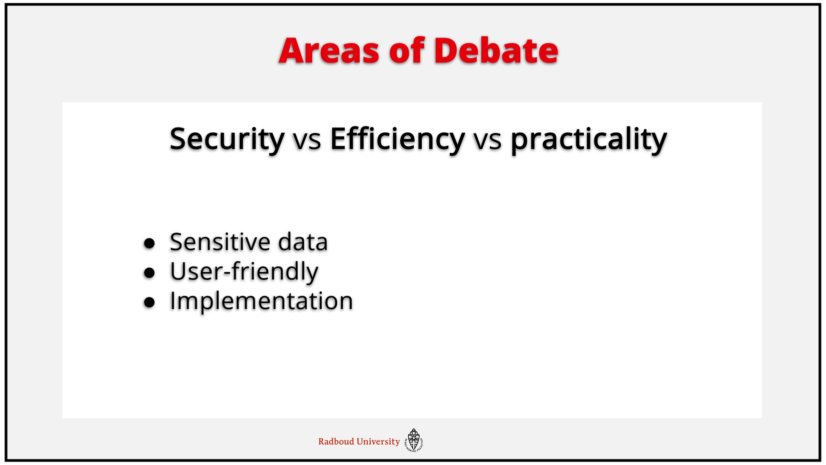


Areas of Debate

Security vs Efficiency vs practicality

- Sensitive data
- User-friendly

96



Areas of Debate

Security vs Efficiency vs practicality

- Sensitive data
- User-friendly
- Implementation

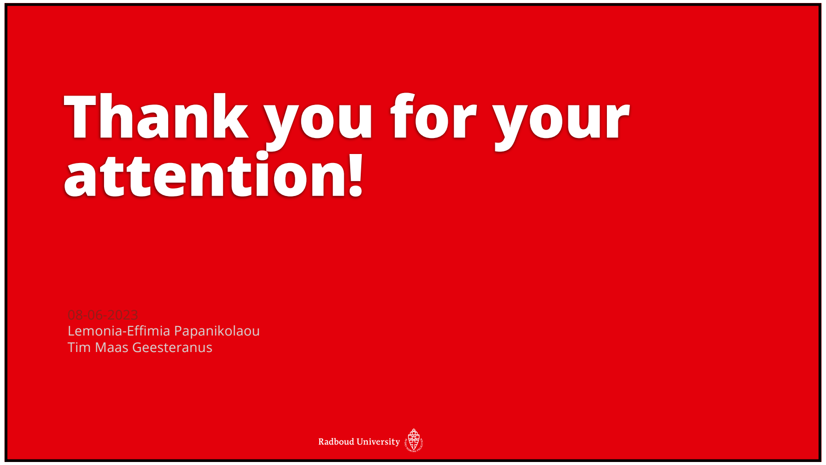
Radboud University

97

So, what do YOU think?

Radboud University

98



Thank you for your attention!

08-06-2023
Lemonia-Effimia Papanikolaou
Tim Maas Geesteranus

Radboud University

99