Roseman Labs

How Multi-Party Computation Unlocks Trusted and Compliant Collaborations in Banking and National Security

Secure Computation Day 2025, Bocconi University

Niek J. Bouman
CTO

European Regulation in Banking

DORA

Digital Operational Resilience Act

AI Act

PSD 3

Payment Services Directive

MiCA

Market in Crypto-Assets Regulation

AMLR

Anti-Money Laundering Regulation
(+ Counter-Terrorism Financing)

European Regulation in Banking

DORA

Digital Operational Resilience Act

AI Act

PSD 3

Payment Services Directive

MiCA

Market in Crypto-Assets Regulation

AMLR

Anti-Money Laundering Regulation
(+ Counter-Terrorism Financing)

European Regulation in Banking

AMLR
Anti-Money Laundering Regulation (effective from July 2027)

Article 75
Exchange of information in the framework of partnerships for information sharing

Article 76
Governs the processing of personal data for AML/CTF purposes

What kind of data could be shared, and why does this makes sense ?

Examples of information exchange:

- Risk scores, e.g. regarding suspicious accounts suspect
- Transactions related to some particular event
- Know-Your-Customer-related data

Why?

- Enrich risk scores with information from other banks
- Decrease false-positive rates
- Better prioritisation of alerts (a pre-processing that boosts productivity of a human analyst)

Why data sharing makes sense: probability theory / information theory perspective

- Let $X \in \{0,1\}$ be the random variable that indicates whether some entity (say, account) is fraudulent
- Let A and B represent the random variables capturing the information held by bank A and B, respectively

Chain rule of mutual information:

$$I(X; A, B) = I(X; A) + I(X; B|A)$$

Information that B knows about X *beyond* what A already knew about X

"Partnerships": Data sharing is often the bottleneck

How to keep multi-stakeholder data safe in such a partnership?
[**Confidentiality**]

"Partnerships": Data sharing is often the bottleneck

How to keep multi-stakeholder data safe in such a partnership?

[**Confidentiality**]

- How to protect against "curious" individuals (employees, sys-admins), security problems at cloud providers, and accidental disclosure of third-party data (e.g. by a human mistake) ?

nrc

BACKGROUND

Bunq employees secretly looked into customer accounts: 'It was too tempting'

Privacy Employees of the Amsterdam online bank bunq looked at salaries of colleagues or spied on ex-lovers. "Everything was always open."

Stijn Bronzwaer, **Merijn Rengers** • June 26, 2024 • Reading time 9 minutes

"Partnerships": Data sharing is often the bottleneck

How to keep multi-stakeholder data safe in such a partnership?

[**Confidentiality**]

- How to protect against "curious" individuals (employees, sys-admins), security problems at cloud providers, and accidental disclosure of third-party data (e.g. by a human mistake) ?

- How to keep the data *use* limited to the consortium-agreed purpose? [**Purpose Binding**]

"Partnerships": Data sharing is often the bottleneck

How to keep multi-stakeholder data safe in such a partnership?
[**Confidentiality**]

- How to protect against "curious" individuals (employees, sys-admins), security problems at cloud providers, and accidental disclosure of third-party data (e.g. by a human mistake) ?
- How to keep the data *use* limited to the consortium-agreed purpose? [**Purpose Binding**]
- How to limit the disclosure of information (only the computed insights vs. the all raw inputs) [**Data Minimisation**]

Data minimisation - metaphor

Input data from multiple data owners

Effective data minimisation

Computational result

Back to Article 75:
How Secure Multi-Party Computation enters the picture

“Obliged entities shall implement appropriate technical and organisational measures, including measures to allows pseudonymisation, to ensure a level of security and confidentiality proportionate to the nature and extent of the information exchanged”

“A data protection impact assessment referred to in Article 35 of Regulation (EU) 2016/679 shall be carried out prior to the processing of any personal data”

Adoption of MPC:
- builds trust among the partnership
- lowers residual risk, accelerating the DPIA

What does this mean for AML collaboration

Encrypted computing (MPC)

- All data is encrypted at the source
- Data remains encrypted at all time
- Combined encrypted data can be analysed
- Banks decide which analyses are allowed
- Only the outcome is shared, with designated party

Example query on encrypted data

Query: is my client connected to entities with a higher risk?

- Via transaction(s), ownership, address-sharing, board members, UBO, etc.

Result:

- How many connections
- Type of connection
- Nature of risk or risk score average
- Transaction volumes

Example use cases in Financial Crime detection

KYC and fraud

Building a distributed list of high-risk accounts / clients, associated with potentially criminal behaviour

Lower risk: leverage intelligence across banks

AML and investigations

Connect higher risk clients and alerts across banks to enable prioritization and faster investigation

Lower costs: prioritization and efficiency in investigations

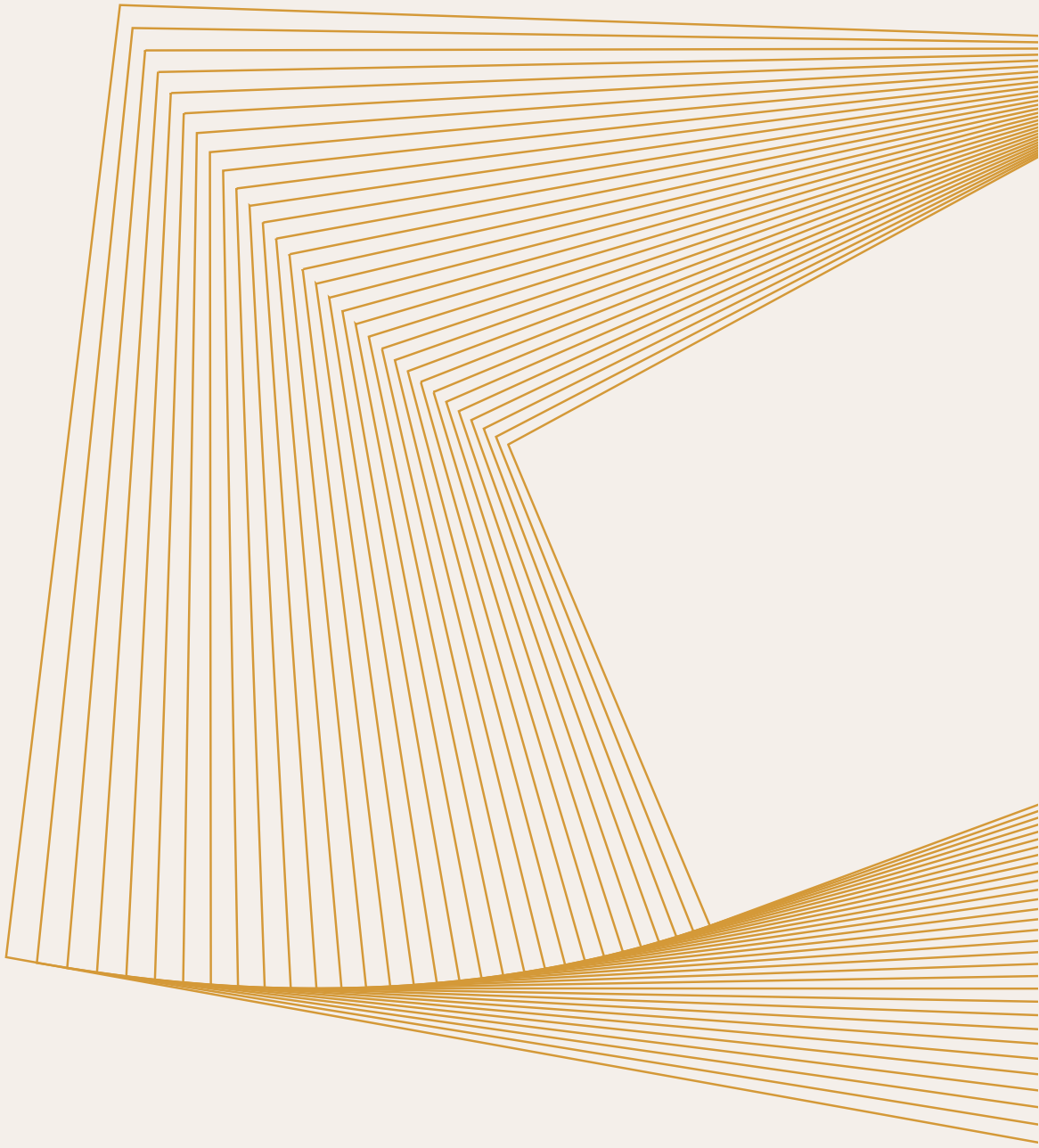
Feedback from FIU

Bring result of FIU investigations back to the banks to learn about results of their Suspicious Activity Reports (SAR filing

Higer quality SARs: establish a feedback loop

Roseman Labs

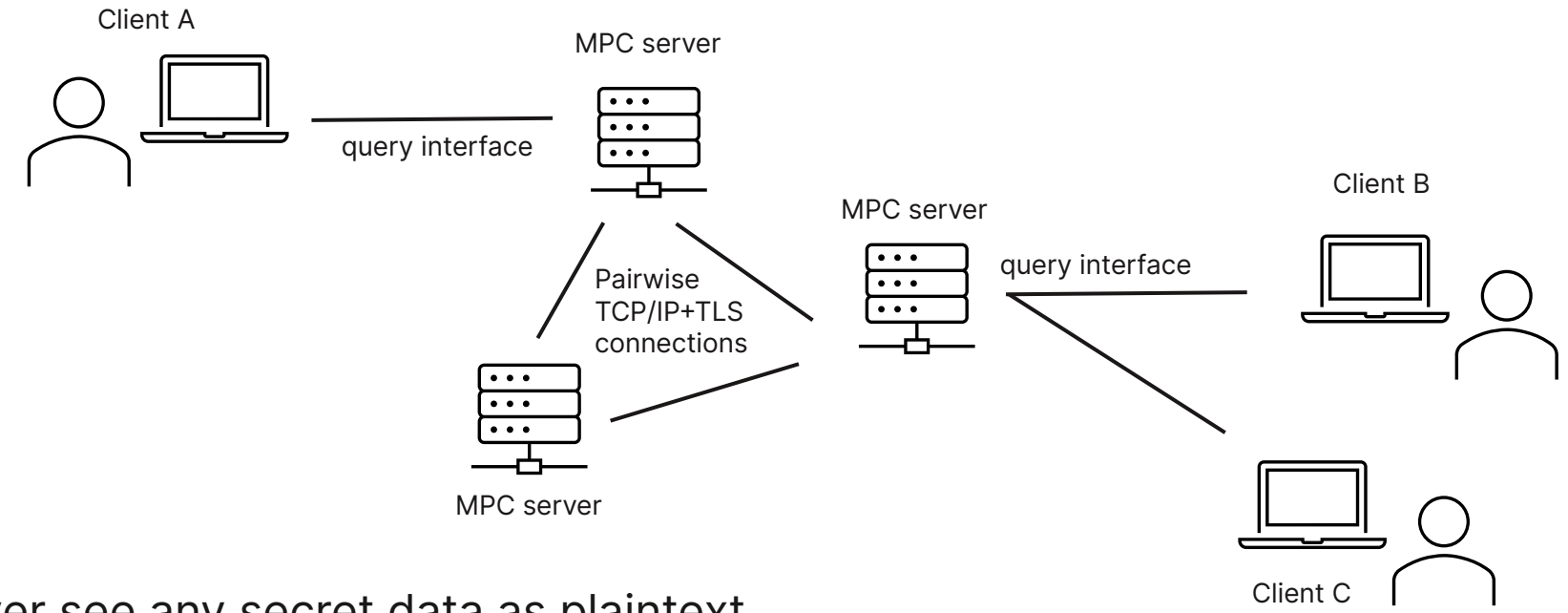
Extract insights from data that you cannot see



Beyond today's security standards

- [x] Encryption at rest
- [x] Encryption in transit
- [x] Encryption in use

Roseman Labs' Encrypted Data Space: System topology and security model



Guarantees

- None of the servers ever see any secret data as plaintext
- Client can only perform queries that have been authorized

Security assumptions

- No collusion between MPC servers

Main benefits of our Encrypted Data Space

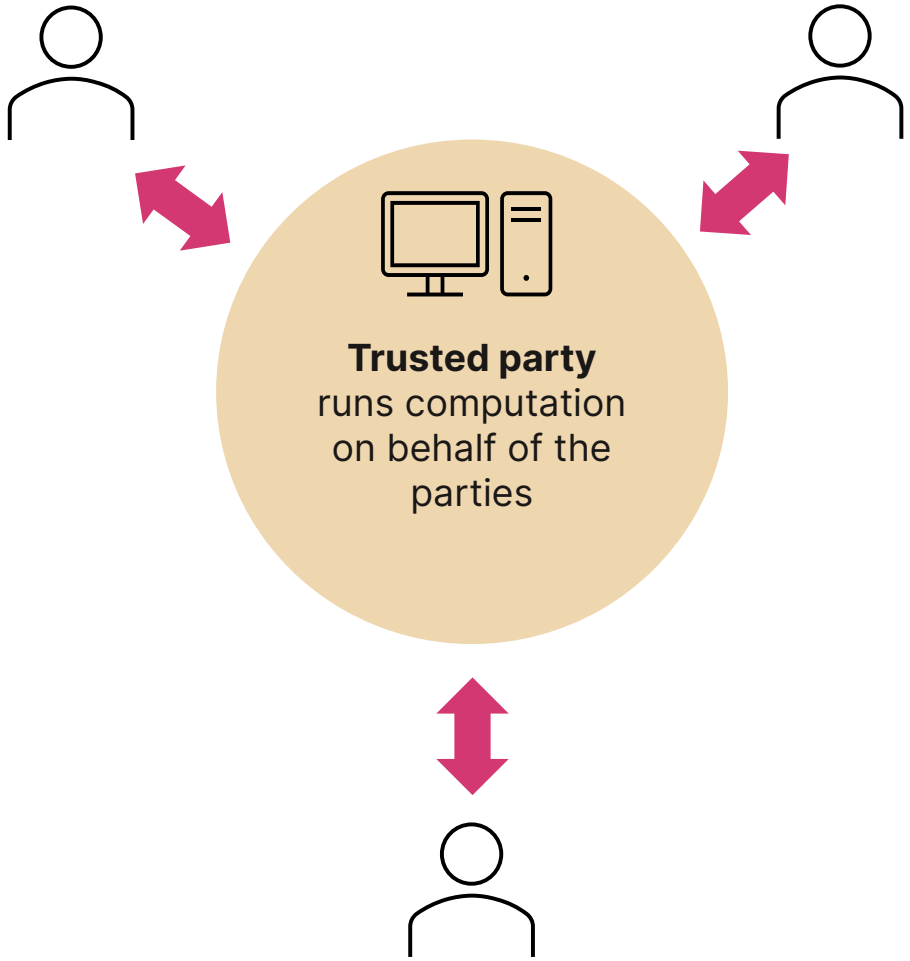
Data minimization

↳ Only reveal results, not the input data

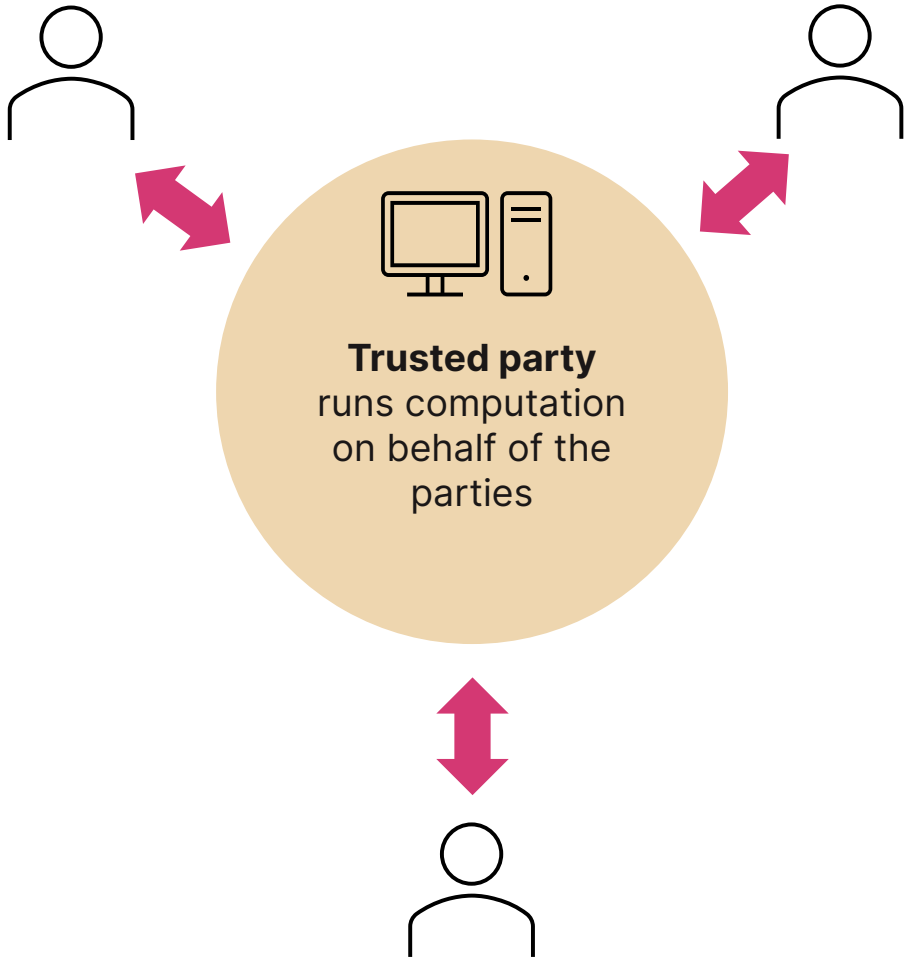
Purpose binding

↳ Owners in control by explicitly approving the analyses

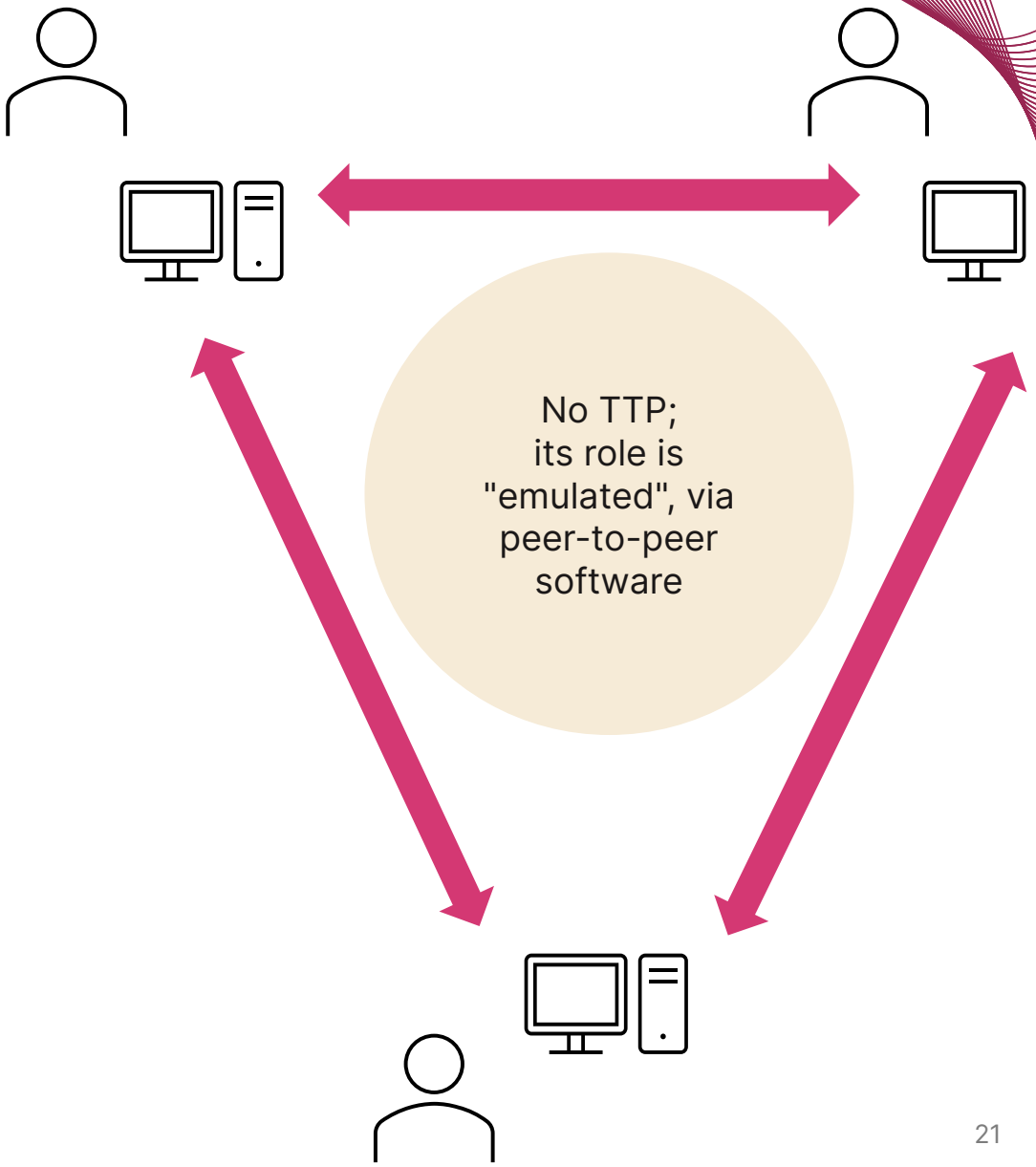
Computation using a Trusted Third Party



Computation using a Trusted Third Party

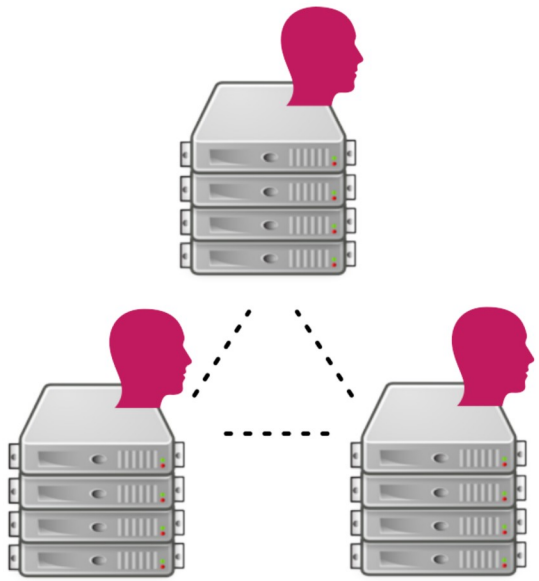


Multi-Party Computation (MPC)



MPC: Deployment alternatives

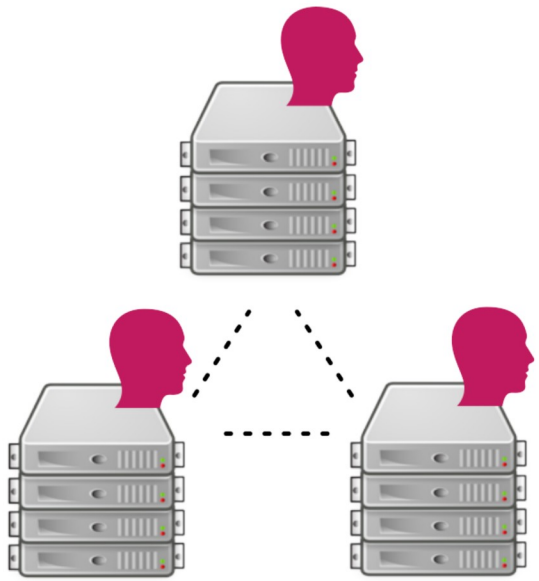
Traditional



Each party manages
its own MPC server

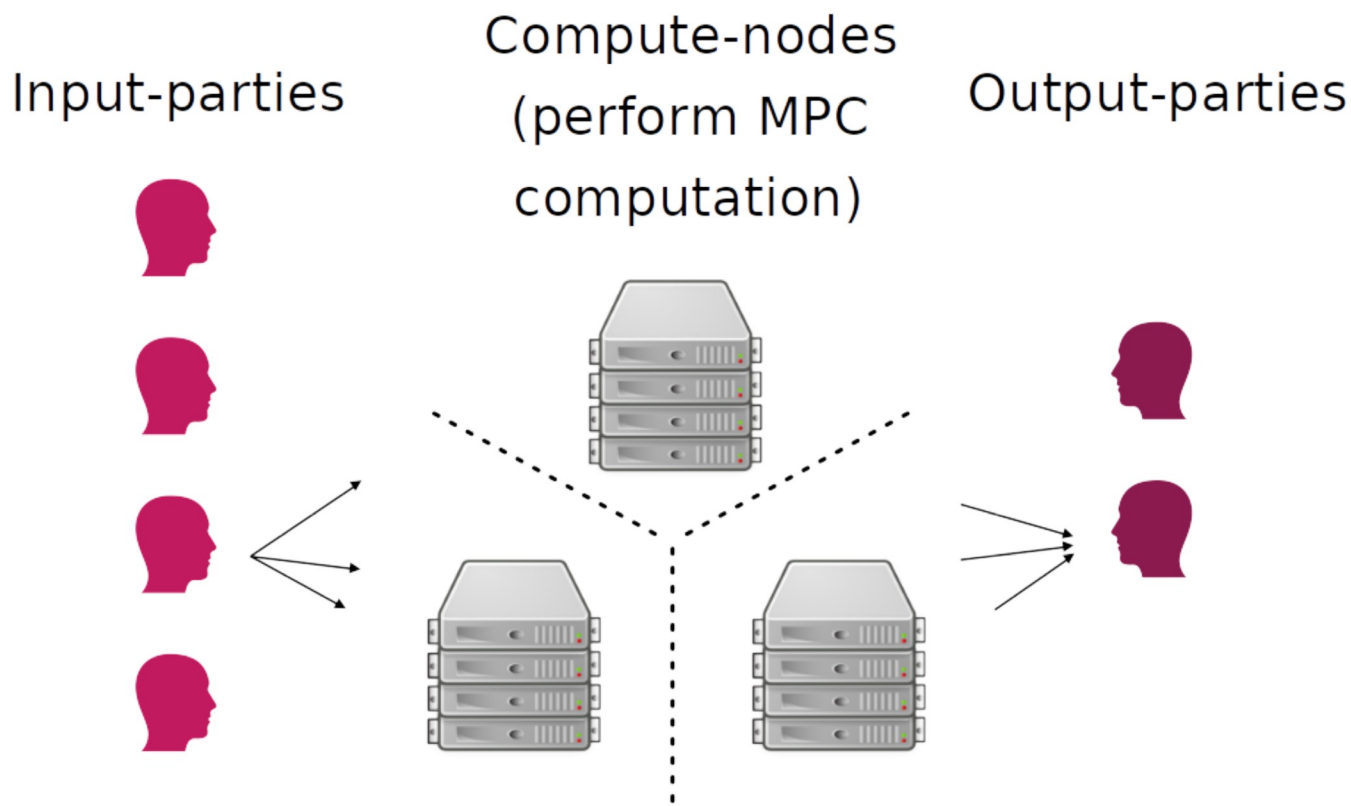
MPC: Deployment alternatives

Traditional

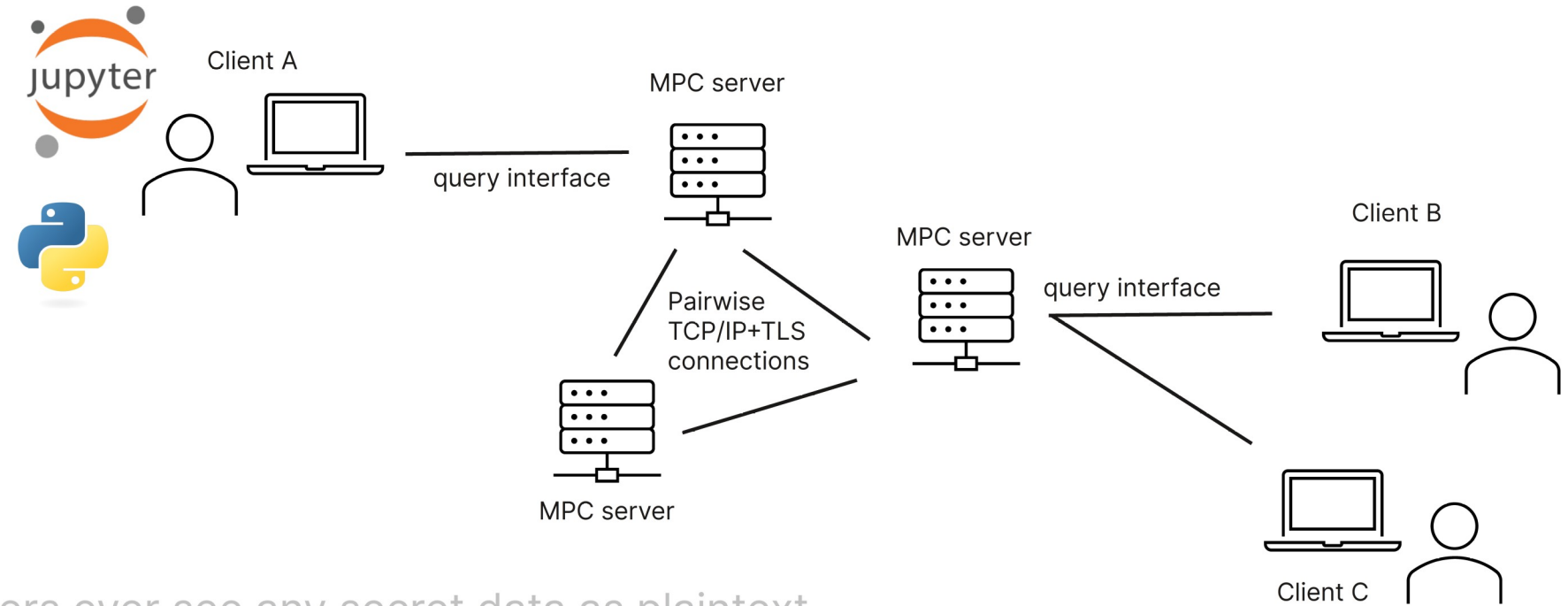


Each party manages
its own MPC server

Delegated + Segregation of duties



Roseman Labs: System topology and security model



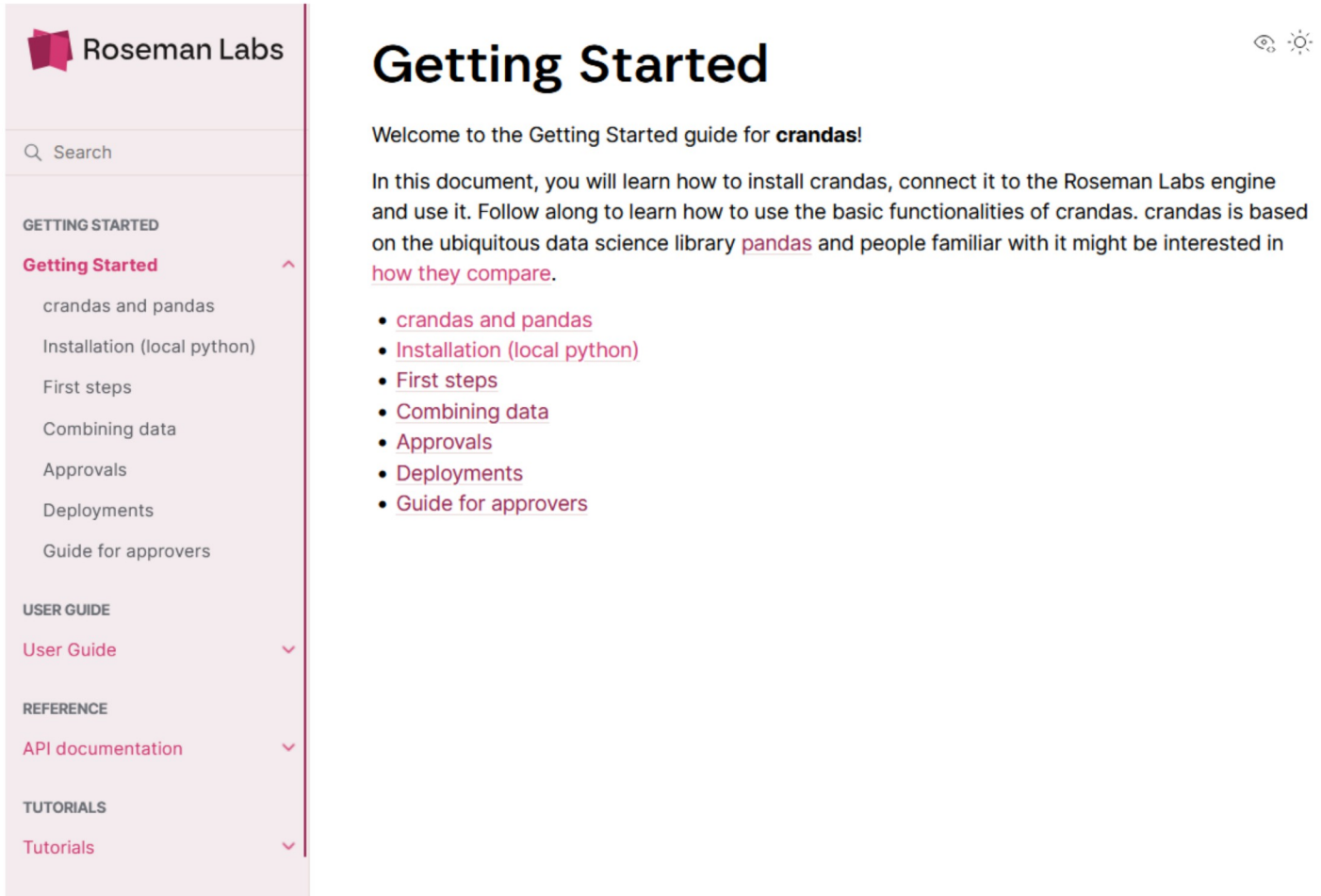
Guarantees

- None of the servers ever see any secret data as plaintext
- Client can only perform queries that have been authorized

Security assumptions

- No collusion between MPC servers

crandas: "Pandas for encrypted data"



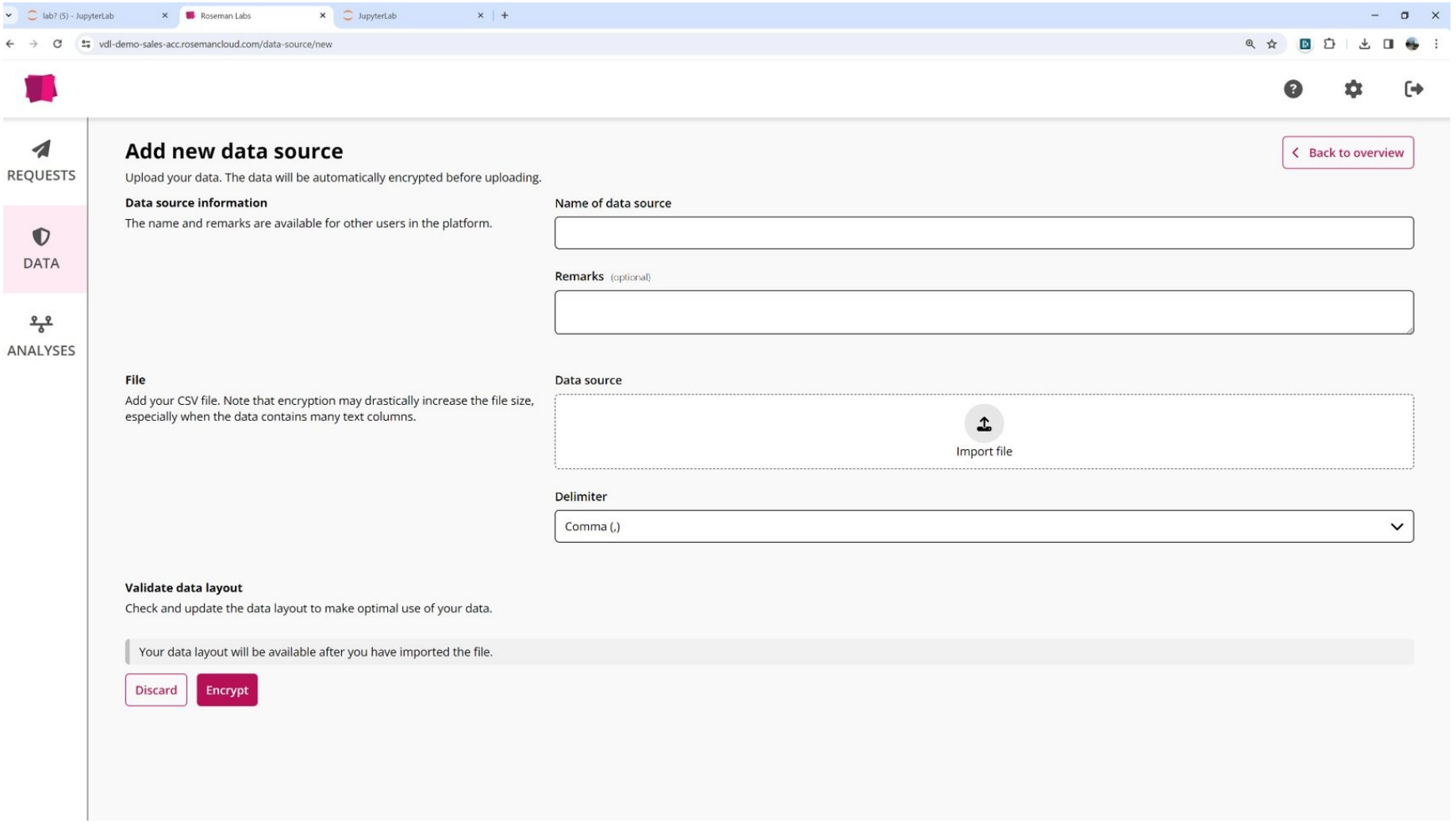
https://docs.rosemanlabs.com/

Share a DataFrame in encrypted form

[54]:
```
titanic=cd.read_csv("titanic.csv")
```

[54]:
```
Handle: 89532C19645AF6A9E68093C211D441A68007A68D07464A98046F121BC9790C3C
Size: 891 rows x 12 columns
CIndex([Col("PassengerId", "i", 1), Col("Survived", "i", 1), Col("Pclass", "i", 1), Col("Name", "s", 83), Col("Sex",
"s", 7), Col("Age", "fp", 1, nullable=True), Col("SibSp", "i", 1), Col("Parch", "i", 1), Col("Ticket", "s", 19), Col("Fa
re", "fp", 1), Col("Cabin", "s", 16, nullable=True), Col("Embarked", "s", 2, nullable=True)])
```

...or alternatively via web-GUI



Your data source has 500 row(s), 11 column(s). After encryption, the file size will be approximately 516.64KB.

INCLUDE	COLUMN NAME	DATA TYPE	ALLOW EMPTY CELLS	INFORMATION
●	name1	Integer	○	There are no data errors in this row.
●	hospital	String	○	There are no data errors in this row.
●	name	String	○	There are no data errors in this row.
●	date_of_birth	Int		
●	sex	Stri		
●	upn	Stri		
●	verrichting_id	Stri		
●	datok	Int		
●	preopgewicht	Integer	○	There are no data errors in this row.
●	blood_pressure	Integer	○	There are no data errors in this row.
●	drug_history	String	○	There are no data errors in this row.

Discard Encrypt

Encrypting data source

Great! Your data source is currently being encrypted. Encrypting your data source can take up to a few minutes. If you have questions or feedback reach out to support@rosemanlabs.com.

Manipulate the encryped DataFrame server-side

[21]:
```
titanic = (titanic
    .project(["Survived", "Pclass", "Sex", "Age", "SibSp", "Parch", "Fare"])
    .dropna()
    .assign(Pclass=lambda x: (x.Pclass-1)/2, Sex=lambda x: x.Sex=="male", Age=lambda x: x.Age/80,
    SibSp=lambda x: x.SibSp/5, Parch=lambda x: x.Parch/6, Fare=lambda x: x.Fare/600))
titanic.describe()
```

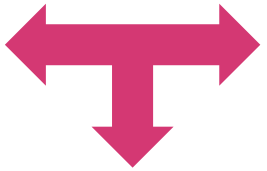
[21]:

	Survived	Pclass	Sex	Age	SibSp	Parch	Fare
type	integer	fixedpoint	integer	fixedpoint	fixedpoint	fixedpoint	fixedpoint
count	714	714	714	714	714	714	714
mean	0.406162	0.618347	0.634454	0.37124	0.102521	0.071895	0.057825
std	0.49146	0.419125	0.481921	0.181582	0.185957	0.142215	0.088201
min	0	0.0	0	0.00525	0.0	0.0	0.0
max	1	1.000002	1	0.999985	1.000004	1.000002	0.854064

Join data sets server-side without decrypting them

`crandas.merge(…)`

ID	Name	Year of birth
13242	Lois	1980
57354	John	1972
32143	Boris	2001
78754	Alice	1993
12321	Francis	1968



ID	Hair color	Body weight
57354	brown	80
76875	black	61
12321	blonde	75
01923	blonde	90
13242	red	102
65764	blonde	55

ID	Name	Year of birth	Hair color	Body weight
13242	Lois	1980	red	102
57354	John	1972	brown	80
12321	Francis	1968	blonde	75

...and apply a decision rule to, or train a ML model on the encrypted (joined) data

```
[9]: features = titanic[["Pclass", "Sex", "Age", "SibSp", "Parch", "Fare"]]
     labels = titanic[["Survived"]]
     model = LogisticRegression()
     model.fit(features, labels)
```

00:49, 100%  00:00 remaining

```
[9]: <crandas.crlearn.logistic_regression.LogisticRegression at 0x7eff7ab336b0>
```

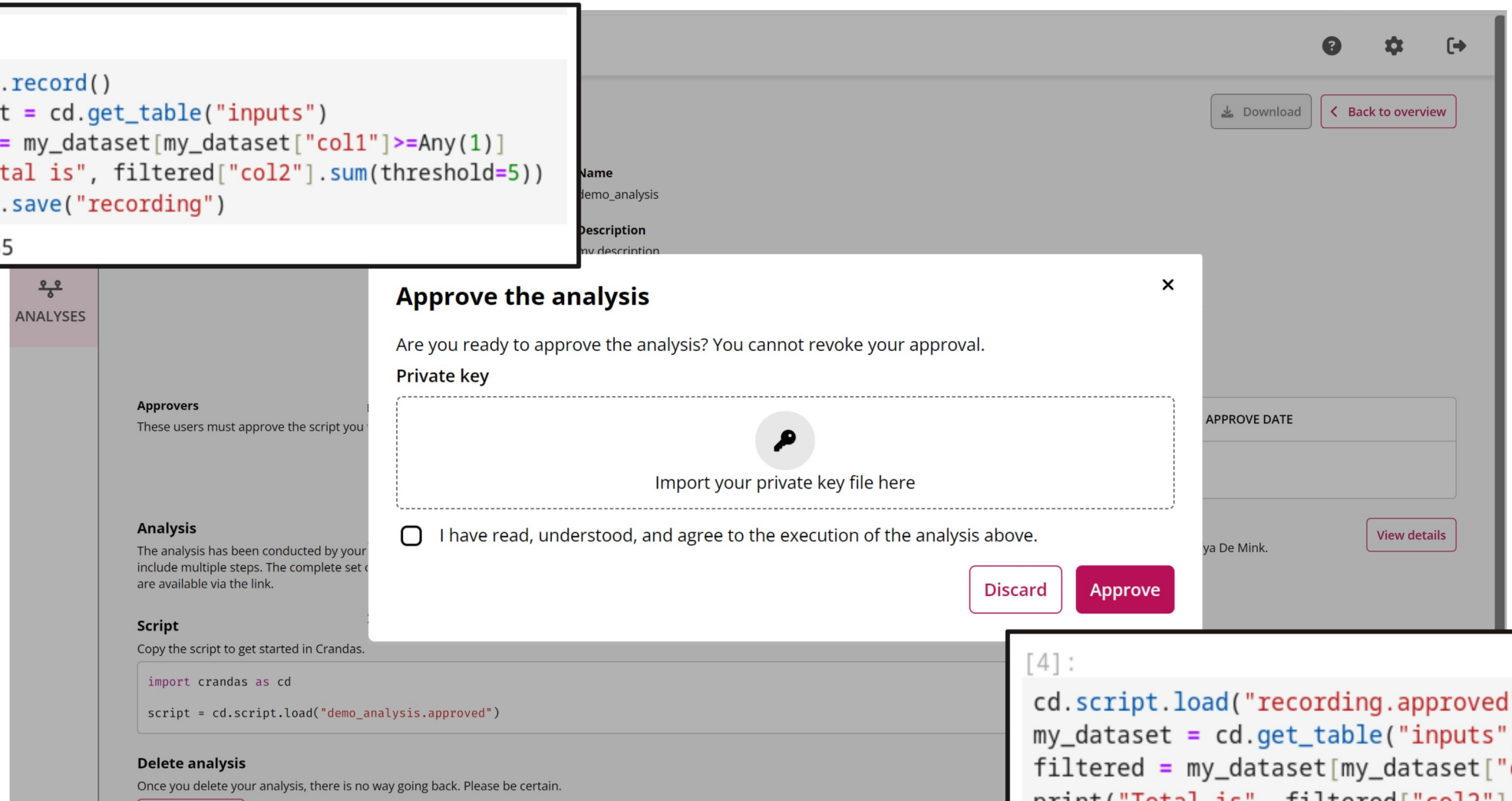
```
[10]: labels_predicted=model.predict(features)
      classification_accuracy(labels, labels_predicted).open()
```

```
[10]: 0.7803277969360352
```

Purpose binding: script approval process

```
[9]:
cd.script.record()
my_dataset = cd.get_table("inputs")
filtered = my_dataset[my_dataset["col1"]>=Any(1)]
print("Total is", filtered["col2"].sum(threshold=5))
cd.script.save("recording")
```

```
Total is 55
```




```
[4]:
cd.script.load("recording.approved")
my_dataset = cd.get_table("inputs")
filtered = my_dataset[my_dataset["col1"]>=4]
print("Total is", filtered["col2"].sum(threshold=5))
```

```
Total is 49
```

Roseman Labs

Use cases & Real-world impact

Collaboration with spotixx

Newsroom

Featured update

Encrypted Computing: The Future of Inter-Bank, Anti-Financial Crime Solutions

June 30, 2025

Financial Services | Partnerships

Roseman Labs

Qorum: a platform to connect financial institutions, combine data, and combat financial crime.

MPC enables collaborative "risk scoring" based on confidential data

Relevant in domains beyond banking

- National security / Police
- Defense
- Cybersecurity

Intelligence Fusion, Secure by Design

Customer Example: NCSC-NL

- → NCSC-NL's **intel-sharing** platform based on Roseman Labs(1)
- → **> 100 partners**, both public and private, share intel regularly – **intel they would not have shared otherwise**
- → **Success**: First take down, partnering to secure Dutch vital infrastructure

(1) Read our publication with NCSC (link)

Winning the 2024 Dutch Privacy Award

“In collaboration with Roseman Labs, Public Transport Groningen Drenthe has been working to find the **best available privacy protection** for analyzing travel behavior without access to personal passenger data from multiple transportation organizations.”
-- Privacy Award Jury

Winning the 2025 Dutch Privacy Award

https://www.youtube.com/watch?v=lphvOKvGiug&t=45s

Gemeente Rotterdam

RosemanLabs
PRIVACY BY DESIGN

Winner application 2025

Municipality of Rotterdam in collaboration with Roseman Labs

Detailed description

The City of Rotterdam is committed to reducing developmental delays among two- and three-year-old toddlers. Research shows that these arrears are hardly caught up in primary education. More than 1,200 toddlers do not participate in pre-school education. It is up to the municipality and its partners (including the Centre for Youth and Family) to gain insight into the problem and adjust quickly.
With the encryption technology of Roseman Labs allows datasets from more than 100 nurseries to be securely linked and analysed without revealing the raw data.

Jury assessment

The collaboration between the Municipality of Rotterdam, Roseman Labs, the Centre for Youth and Family and the day-care centres demonstrates that innovative privacy technologies can be used effectively to address societal challenges, while maintaining privacy protection.

Roseman Labs

Thanks! Questions?

Roseman Labs

How we can help you?

info@rosemanlabs.com
niek.bouman@rosemanlabs.com