Agora Cloud Event, June 2024

Privacy-Preserving Machine Learning

ZAMA

Zama is a **cryptography company** providing **open source homomorphic encryption solutions** for **blockchain and AI.**

Founded in 2020 in Paris

80 people, including 50 in France and 75 in EU

23 patents

73 M€ in funding (including from BPI)

Privacy-Preserving Machine Learning

Security breaches

Breaches

Pattern

	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Basic Web Application Attacks	12	1	10	30	30	161	55	124	71	12	21	113	76	21	30	22
Denial of Service	1						1							1		
Everything Else	1	1		13		12	8	1	6	1		3	32		15	4
Lost and Stolen Assets				21	2	18	24	4	7		11	22	64	7	1	
Miscellaneous Errors	2	1	5	375	86	270	585	84	154	20	185	238	493	140	10	18
Privilege Misuse	6		4	97	39	63	266	38	68	12	45	71	86	41	5	5
Social Engineering	35	7	158	764	79	251	141	116	190	47	71	500	119	118	119	35
System Intrusion	52	12	43	860	70	427	168	250	373	64	90	409	245	78	201	59

Action

	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Environmental	1								1							
Error	3	1	5	393	88	280	588	87	161	20	195	255	551	144	10	18
Hacking	66	11	172	872	119	598	204	315	405	94	110	603	341	126	204	84
Malware	50	11	43	881	71	457	165	277	379	77	94	429	292	79	215	65
Misuse	7		4	97	39	63	266	38	69	12	45	74	86	41	5	5
Physical	2			3		8	5	1	1			5	3	2	13	
Social	37	7	158	764	79	261	142	117	190	47	71	504	119	118	121	37

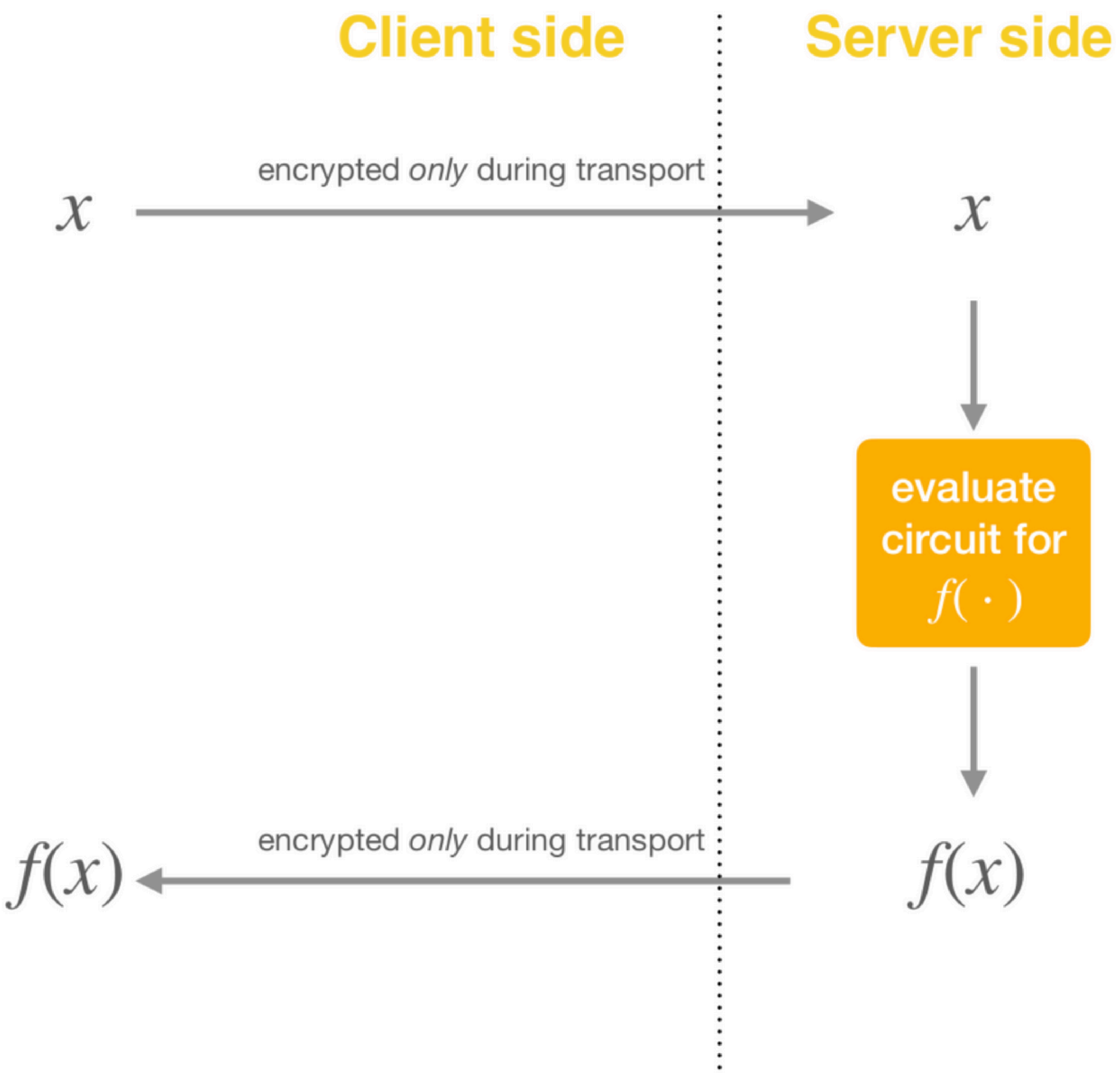
Asset

	Accommodation (72)	Administrative (56)	Construction (23)	Education (61)	Entertainment (71)	Finance (52)	Healthcare (62)	Information (51)	Manufacturing (31-33)	Mining + Utilities (21+22)	Other Services (81)	Professional (54)	Public Administration (92)	Real Estate (53)	Retail (44-45)	Transportation (48-49)
Embedded																
Kiosk/Term						5									9	
Media			3	89	10	71	238	6	46	5	44	68	197	22	1	
Network						4	3	1	2				1		2	
Person	37	7	158	764	79	262	142	118	190	47	71	505	119	119	121	37
Server	92	20	211	1,228	232	914	601	473	641	108	271	1,032	586	279	323	109
User Dev	11	2	4	51	16	77	55	76	53	28	43	108	111	8	35	14

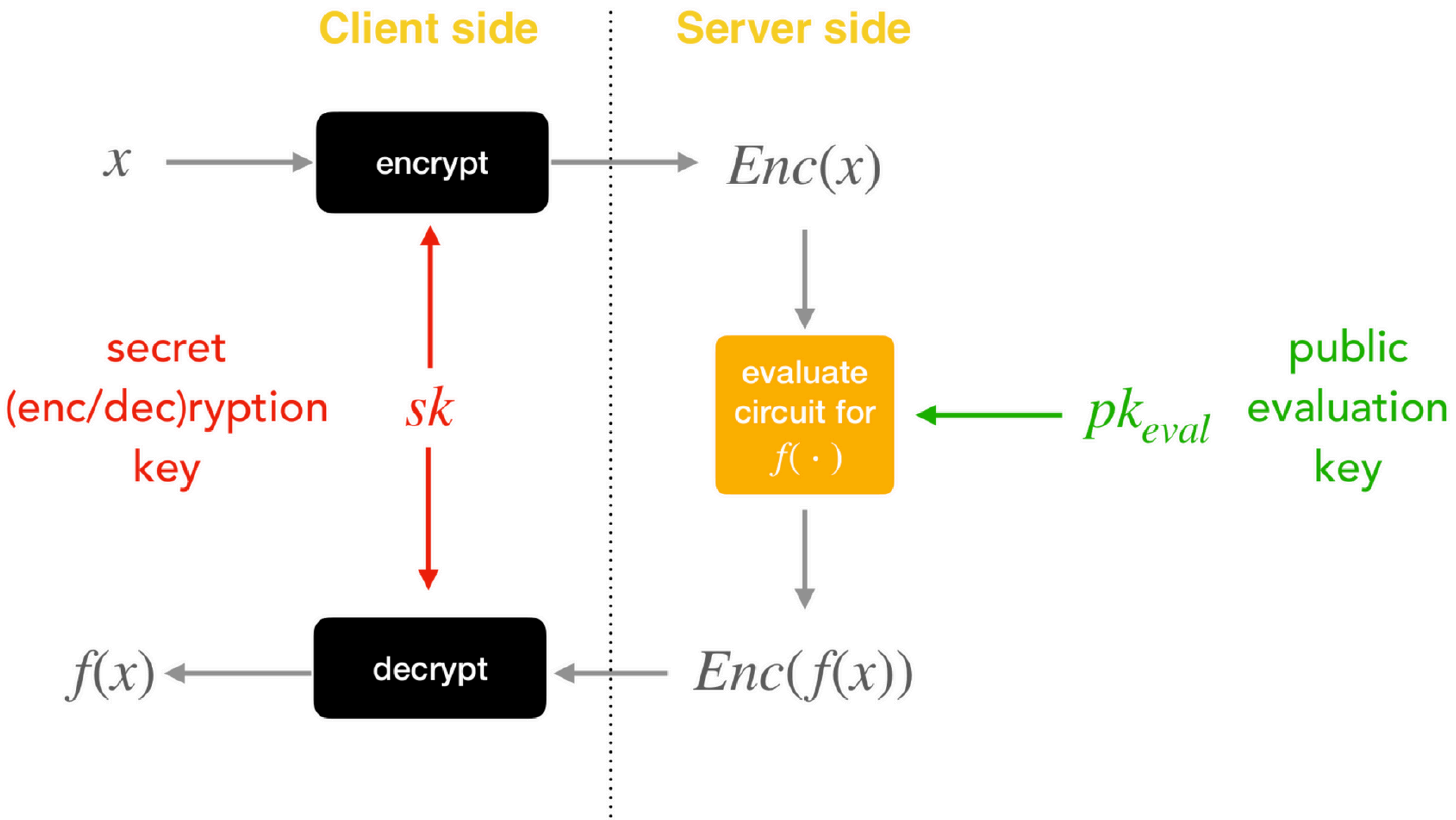
0% 25% 50% 75% 100%

Source: https://www.verizon.com/business/resources/reports/dbir/

Data is encrypted only during the transport



With FHE, the data remains encrypted during processing



Typical use cases where privacy is needed

Healthcare

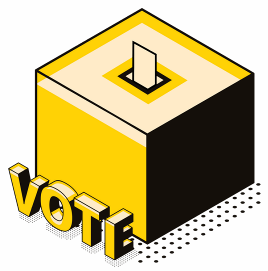
Enable private AI diagnostics and collaborative R&D

Advertising

Match privacy-preserving ad based on encrypted profiles

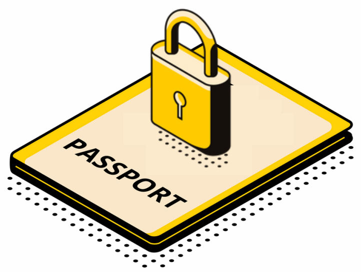
Defense

Collaborate between agencies without revealing secrets



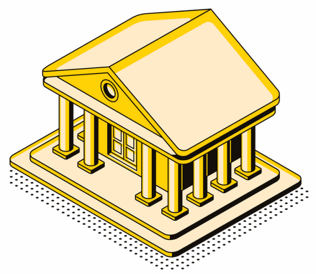
Government

Digitalize government services without trusting cloud providers



Biometrics

Authenticate users without revealing their real identities



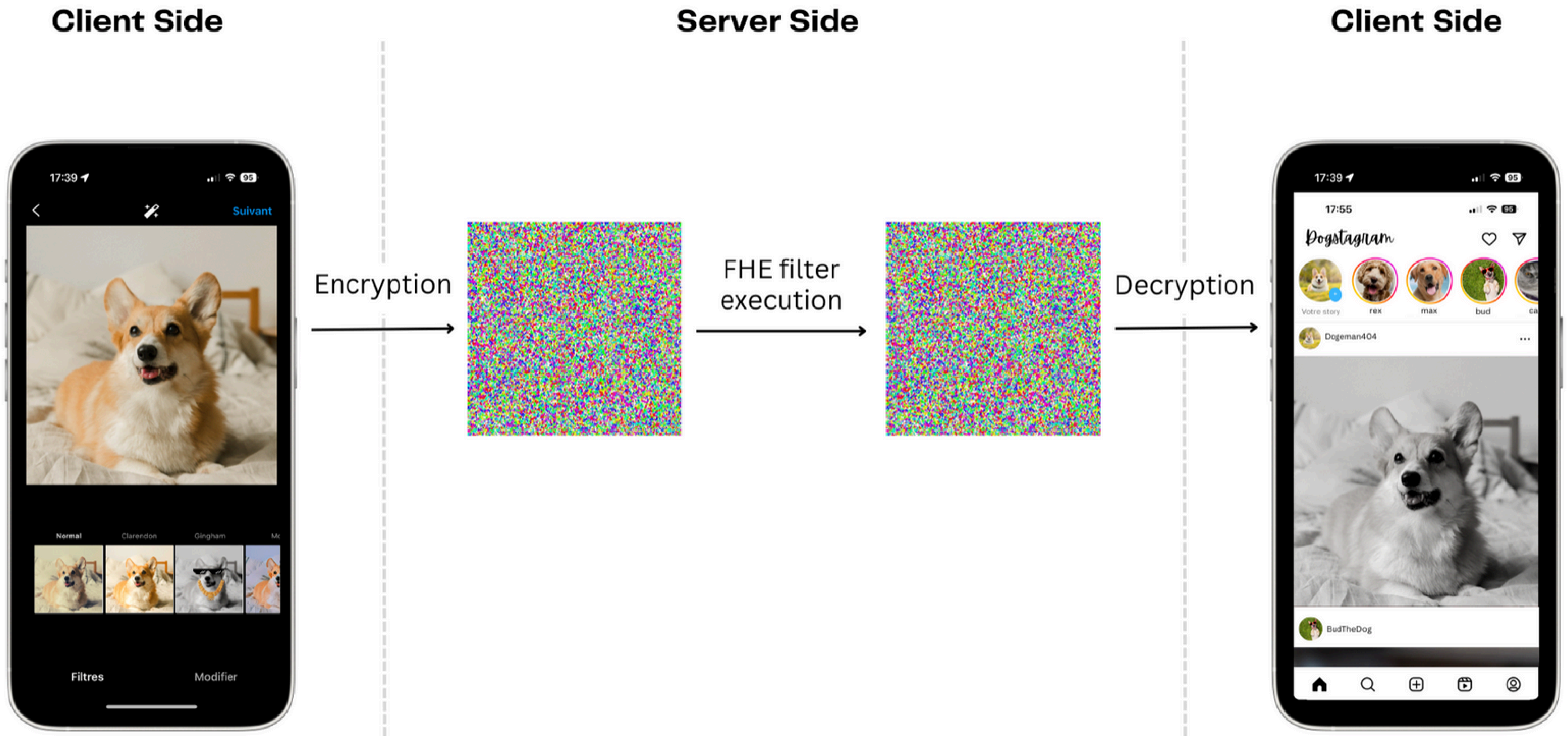
Finance

Enable confidential credit scoring, dark pools and more

We are open-source

- **Libraries**
  Everything is available on Zama's Github repo: zama-ai
- **Free for research and prototype**
  Our libraries are free for research and prototype. It's only when used in commercial products that licenses change
- **Bounties**
  We encourage people to showcase some use-cases with our Bounty Program: github.com/zama-ai/bounty-and-grant-program
- **Demos**
  We show our own examples, including on our Hugging Face: zama-fhe
- **Ecosystem**
  We build an ecosystem around FHE, by helping companies and granting them. Also we co-build fhe.org
- **Community support**
  We offer free support to users on Discord: discord.com/invite/fhe-org

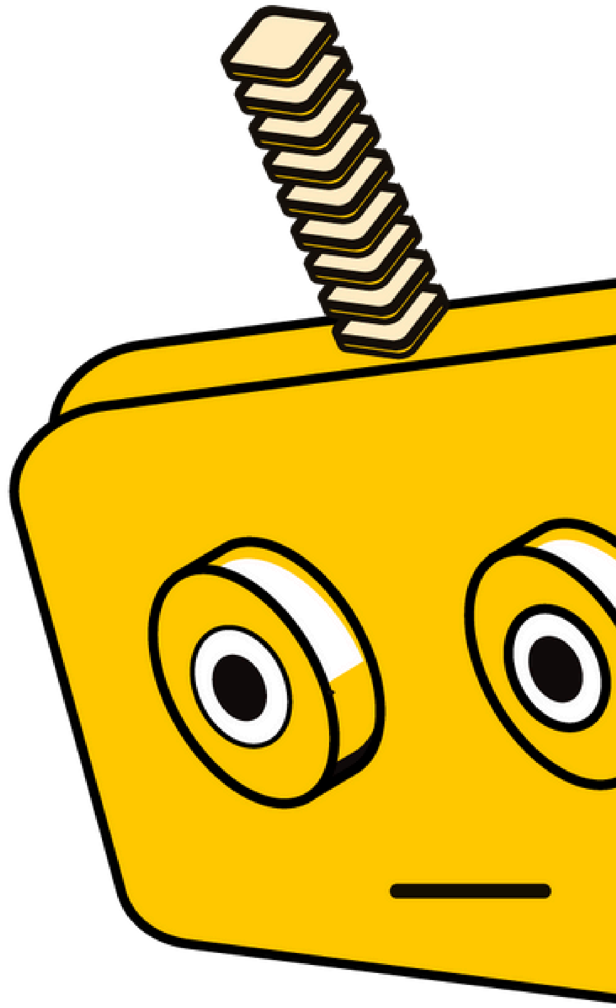
Image filtering as a demo



https://huggingface.co/spaces/zama-fhe/encrypted_image_filtering

Concrete ML

- Linear Models
- Tree-Based Models
- Neural Networks
- Large Language Models
- Dataframes
- Confidential training
- Collaborative compute
- Model IP protection



Privacy-Preserving ML

Our APIs are already familiar

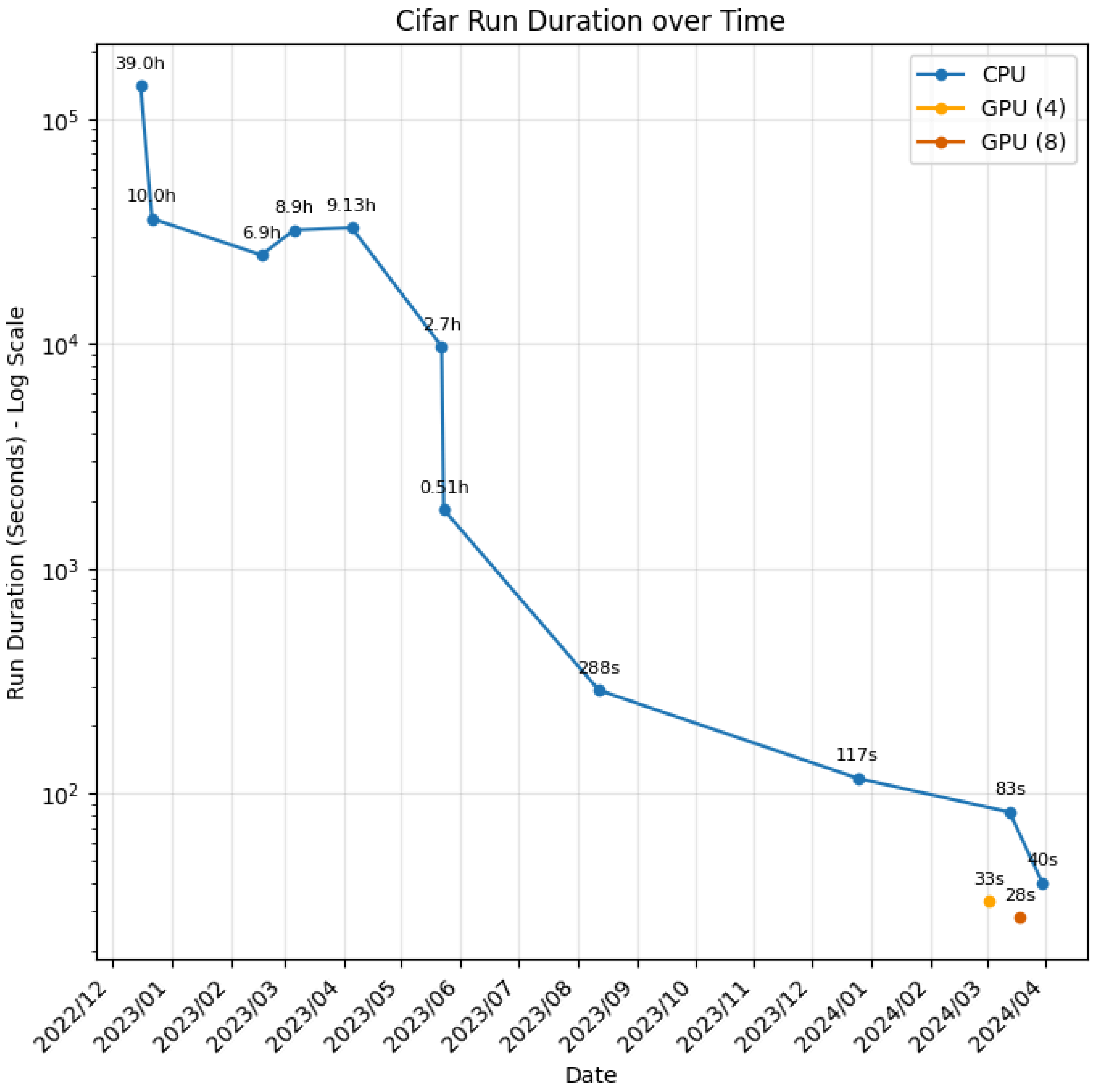
```python
from concrete.ml.sklearn import LogisticRegression

model = LogisticRegression(n_bits=12)
model.fit(X_train, y_train)
model.predict(X_test)
model.compile(X_train)
model.predict(X_test, fhe="simulate")
model.predict(X_test, fhe="execute")
```

```python
from concrete.ml.sklearn import XGBClassifier

model = XGBClassifier(n_bits=8)
model.fit(X_train, y_train)
model.predict(X_test)
model.compile(X_train)
model.predict(X_test, fhe="simulate")
model.predict(X_test, fhe="execute")
```

```python
import torch
import torch.nn as nn
import torch.nn.functional as F
from concrete.ml.torch.compile import compile_torch_model

class SimpleNet(nn.Module):
    def __init__(self):
        super().__init__()
        self.fc1 = nn.Linear(784, 30)
        self.fc2 = nn.Linear(30, 30)
        self.fc3 = nn.Linear(30, 2)

    def forward(self, x):
        x = F.relu(self.fc1(x))
        x = F.relu(self.fc2(x))
        x = self.fc3(x)
        return x

model = SimpleNet()
input_data = torch.randn(100, 784)

quantized_fhe_module = compile_torch_model(model, input_data, n_bits=8)
```

Privacy-Preserving ML

FHE is getting faster and faster



Comparison with other PETs

	Concrete ML	Other FHE	MPC (multi party computation)	TEEs (trusted execution environment)
Models supported				
Layers supported				
Performance				
Computation result				
Hardware acceleration				
Developer experience				
Security				

Comparison with other PETs

	Concrete ML	Other FHE	MPC (multi party computation)	TEEs (trusted execution environment)
Models supported				Anything
Layers supported				
Performance				Fast
Computation result				Exact
Hardware acceleration				Yes
Developer experience				Medium
Security				Prone to side channel attacks

Comparison with other PETs

	Concrete ML	Other FHE	MPC (multi party computation)	TEEs (trusted execution environment)
Models supported			Limited due to large communication	Anything
Layers supported				
Performance			Fast	Fast
Computation result			Exact	Exact
Hardware acceleration			No	Yes
Developer experience			Hard	Medium
Security			Nodes can collude to reveal the data	Prone to side channel attacks

Comparison with other PETs

	Concrete ML	Other FHE	MPC (multi party computation)	TEEs (trusted execution environment)
Models supported		Limited depth	Limited due to large communication	Anything
Layers supported		Basic support for non-linear layers		
Performance		Medium to fast depending on the model	Fast	Fast
Computation result		Approximate	Exact	Exact
Hardware acceleration		Yes	No	Yes
Developer experience		Hard	Hard	Medium
Security		No known attack	Nodes can collude to reveal the data	Prone to side channel attacks

Comparison with other PETs

	Concrete ML	Other FHE	MPC (multi party computation)	TEEs (trusted execution environment)
Models supported	Anything	Limited depth	Limited due to large communication	Anything
Layers supported		Basic support for non-linear layers		
Performance	Medium to fast depending on the model*	Medium to fast depending on the model	Fast	Fast
Computation result	Exact and Approximate	Approximate	Exact	Exact
Hardware acceleration	Yes	Yes	No	Yes
Developer experience	Simple	Hard	Hard	Medium
Security	No known attack	No known attack	Nodes can collude to reveal the data	Prone to side channel attacks

*ASIC acceleration for Concrete ML will be available in 2025 and offer up to 1000x speedup

HTTPZ

Thank you.

ZAMA

Privacy-Preserving ML

Contact and Links

benoit.chevalliermames@zama.ai

zama.ai

github.com/zama-ai

community.zama.ai/

discord.fhe.org

ZAMA