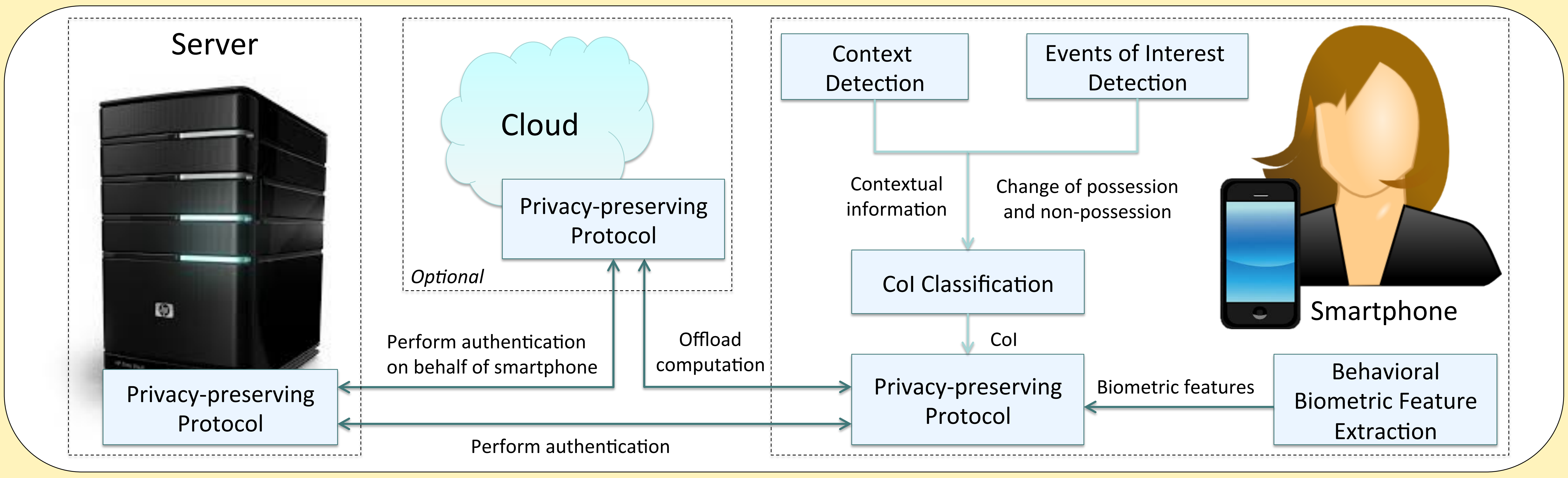
Energy-Efficient Privacy-Preserving Active Authentication of Smartphone Users

PIs: **Paolo Gasti**, NYIT; **Kiran Balagani**, NYIT; **Gang Zhou**, College of William and Mary

https://lamp.soecs.nyit.edu/w/index.php/projects/

Motivation

- Biometric templates represent sensitive information
- Storing them on smartphones is risky, as they can be exposed when the adversary gains physical access to the device
- Cancelable biometrics and BKG offer limited protection when biometric traits have low entropy
- Strong biometric templates on remote servers and authenticating via current privacy-preserving protocols is too expensive



Server

Privacy-preserving Protocol

Cloud

Privacy-preserving Protocol

Optional

Perform authentication on behalf of smartphone

Offload computation

Perform authentication

Context Detection

Events of Interest Detection

Contextual information

Change of possession and non-possession

CoI Classification

CoI

Privacy-preserving Protocol

Biometric features

Behavioral Biometric Feature Extraction

Smartphone

Approach

1. Make privacy-preserving authentication sustainable on smartphones
   - Reduce energy consumption of protocol components
   - Outsource computation to untrusted third-party (e.g., VM in the cloud)
2. Authenticate only when needed
   - Detect events of interests, such as change of possession and non-possession

Technical Approach

Detection of events of interest

- Focus on detecting events that indicate need to re-authenticate, rather than detecting events that allow postponing authentication
  - *Change of possession* events
  - *Non-possession* events
- Use events to build *confidence on identity*

Energy efficient privacy-preserving protocols

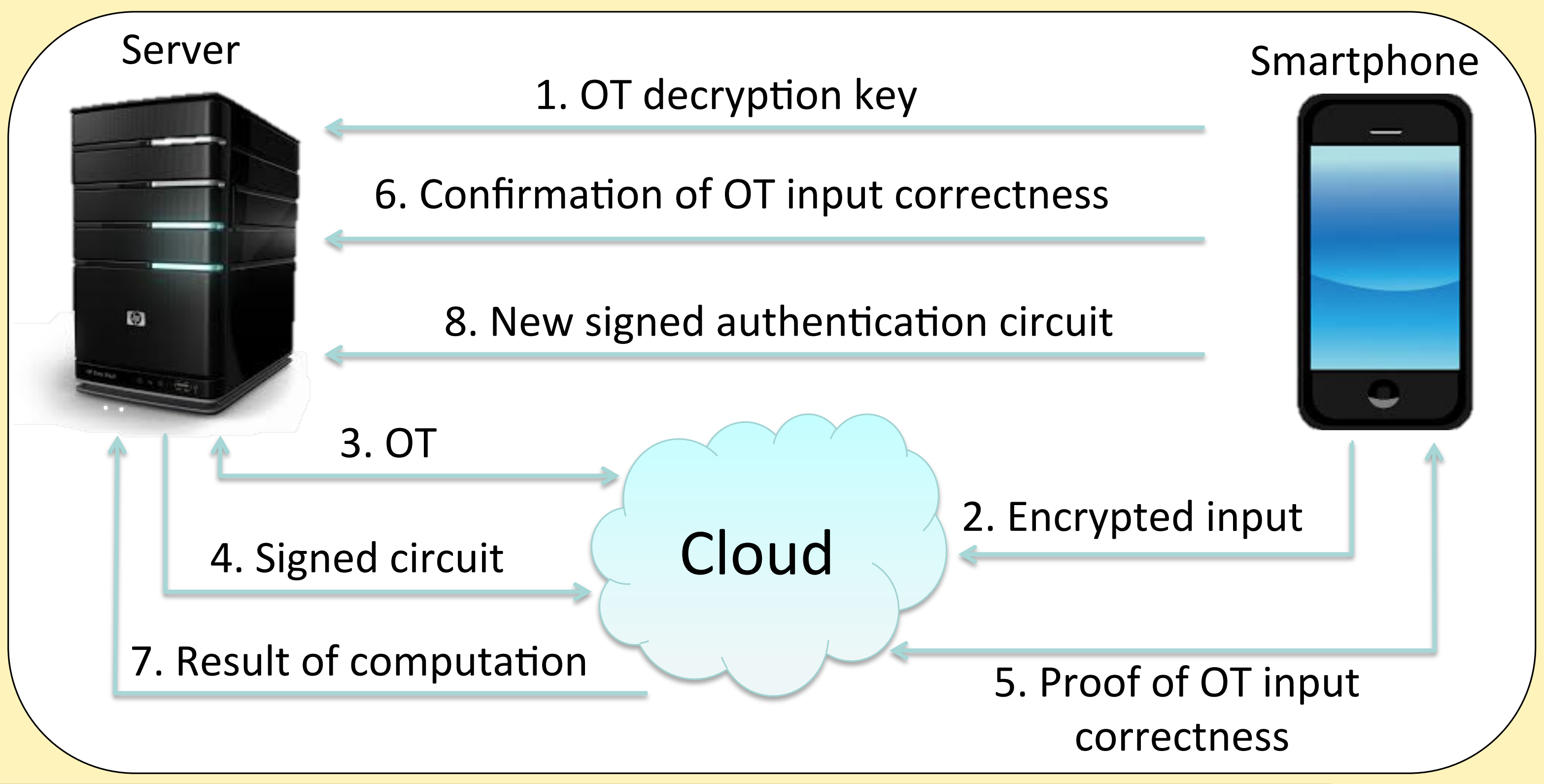
- Reorganize communication and computation in uniform blocks
- Minimize data exchanged over network
- Leverage confidence on identity to securely and efficiently outsource computation to untrusted party

Preliminary results on outsourcing computation

Scaled Manhattan Distance, 28 features

	Time on Smartphone (s)	Bandwidth on Smartphone (MB)	Energy	# of Protocol Runs
GC (semi-honest)	1.80	0.15	0.76	1,300
GC (malicious)	378.69	21.78	274.87	35
Our work (malicious)	**0.6**	**0.02**	**0.2**	**>48k**

	1,600-bit Input		16,384-bit Input	
	Time (s)	Bandwitdh (MB)	Time (s)	Bandwitdh (MB)
Whitewash	95.57	23.56	941.15	241.02
CMTB	453.36	41.05	1,335.75	374.03
Our work	**3.29**	**0.49**	**24.97**	**4.24**



Server

Smartphone

1. OT decryption key

6. Confirmation of OT input correctness

8. New signed authentication circuit

3. OT

2. Encrypted input

4. Signed circuit

Cloud

7. Result of computation

5. Proof of OT input correctness

Interested in meeting the PIs? Attach post-it note below!

National Science Foundation
WHERE DISCOVERIES BEGIN

NSF Secure and Trustworthy Cyberspace Principal Investigator Meeting
Jan. 9 - 11th 2017
Arlington, VA