BETA: Biometric Enabled Threshold Authentication

Saikrishna Badrinarayanan

(Visa Research)

Joint work with

Shashank Agrawal
Western Digital

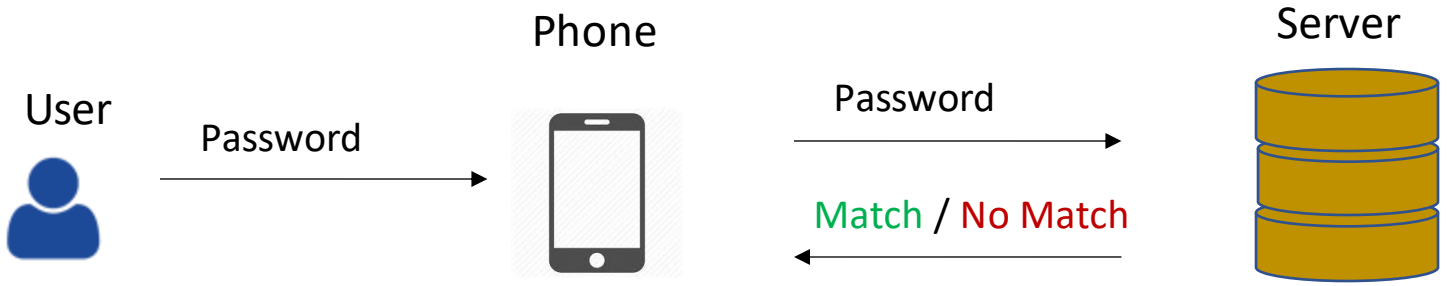
Payman Mohassel
Facebook

Pratyay Mukherjee
Visa Research

Sikhar Patranabis
Visa Research

Password-based Authentication

- Enrollment phase
  - Enroll password on the server – store salted hash
- Online phase



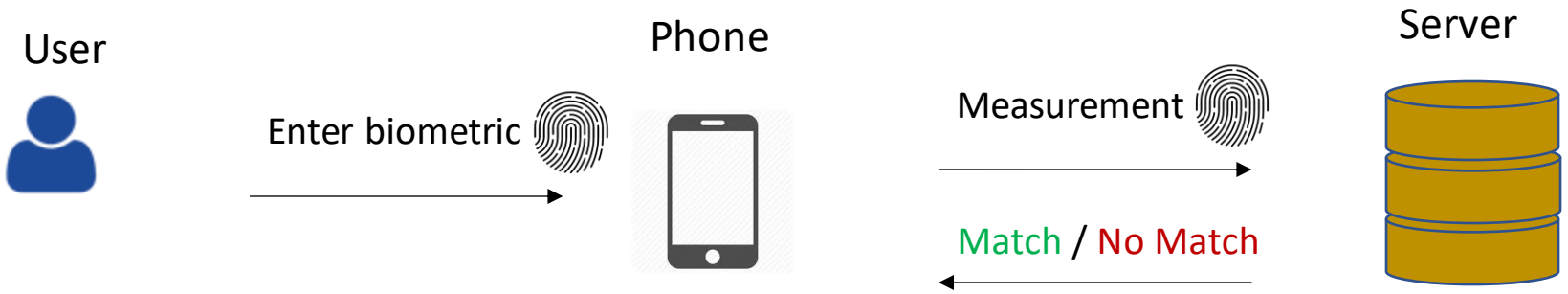
Issues

- Offline dictionary attacks - Large scale real world breaches
- Usability concerns: High entropy requirement

Biometric Authentication

- Enrollment phase
  - store biometric template on a server

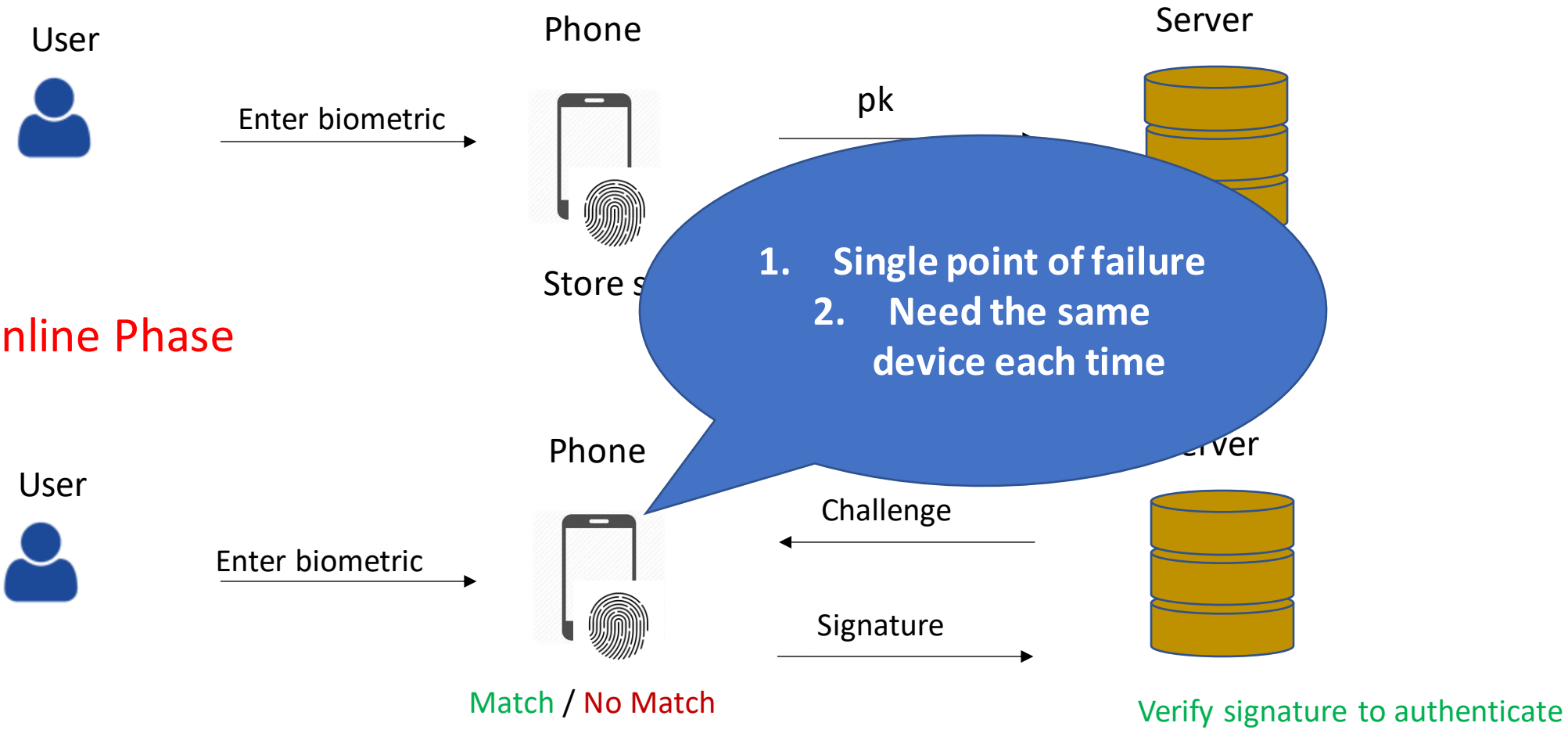
- Online phase



- Better usability than passwords
- Server side breaches are more damaging

FIDO protocol and how it works

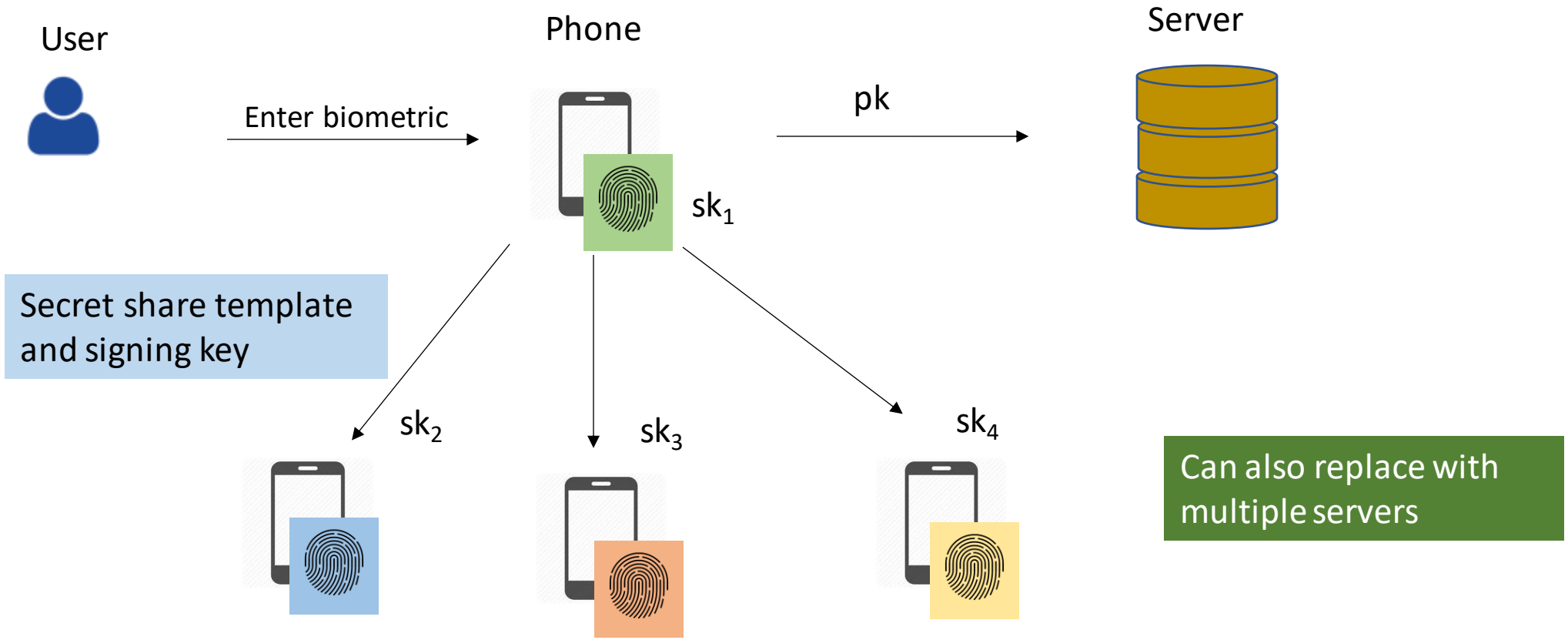
- Enrollment phase



- Online Phase

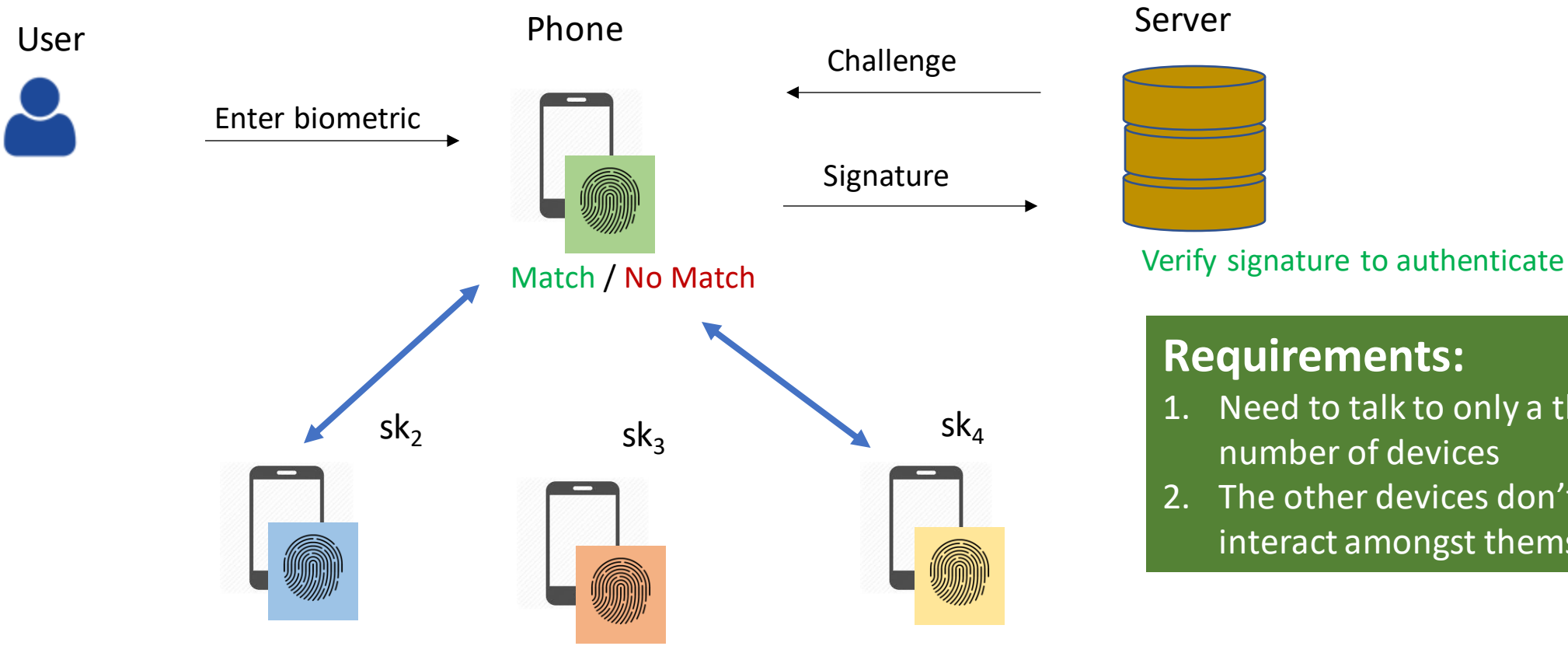
``Distributed" FIDO

- Enrollment phase



``Distributed" FIDO

- Online phase



Requirements:

1. Need to talk to only a threshold number of devices
2. The other devices don't need to interact amongst themselves.

Our Results

- New Primitive: Fuzzy Threshold Tokenizer
- Formal security model with universally composable (UC) security

- Two feasibility results for any biometric matching metric and arbitrary corruption threshold.
- Efficient protocol for Cosine Similarity (Face/Fingerprint recognition) tolerating single corruption.

Thank you!

Paper at
ia.cr/2020/679