TECHNISCHE
UNIVERSITÄT
DARMSTADT

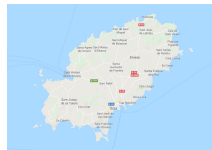
TU Graz

SCIENCE
PASSION
TECHNOLOGY

Mobile Private Contact Discovery

Daniel Kales Christian Rechberger (TU Graz)

Matthias Senker Thomas Schneider Christian Weinert (TU Darmstadt)

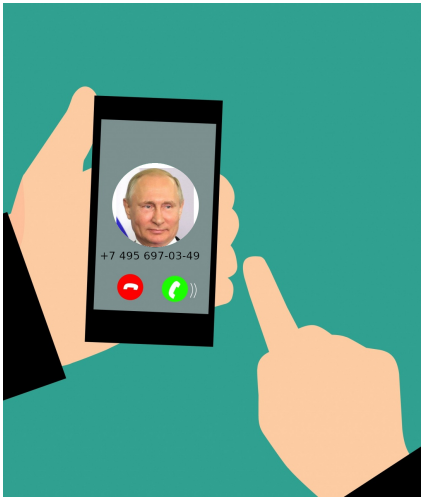


Ibiza

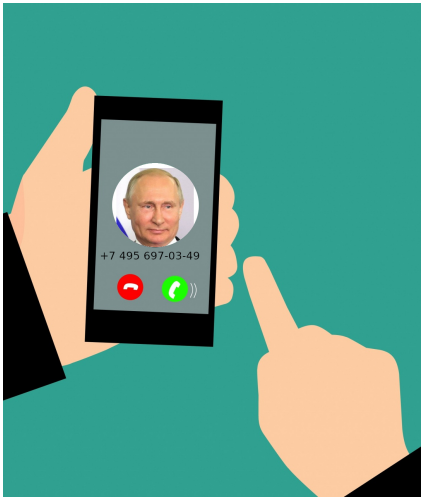
Mobile Private Contact Discovery

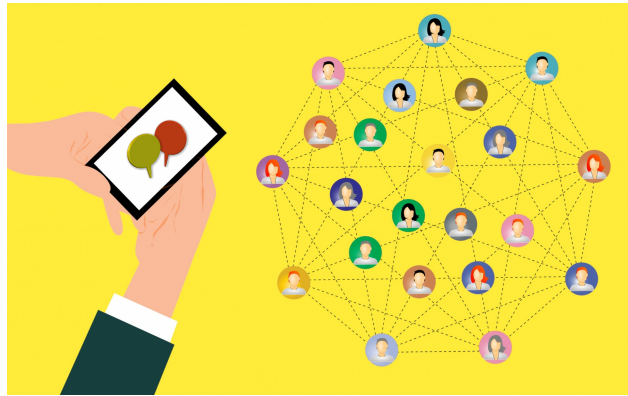
Ibiza

Mobile Private Contact Discovery

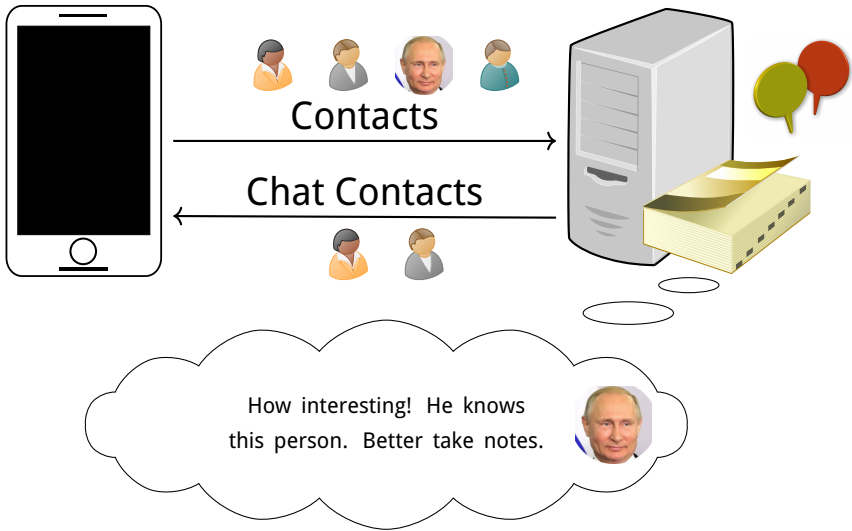


Mobile Private Contact Discovery





Mobile Private Contact Discovery



Mobile Contact Discovery

- Current Solution: Naive Hashing
  - Employed by some existing messengers
  - Vulnerable to brute-force
  - Salting only marginal help

Messenger	Hashed	Salted
Confide	✓	✗
Dust	✗	✗
Eleet	✗	✗
Signal (legacy)	✓	✗
SIMSme	✓	✓
Telegram	✗	✗
Threema	✓	✗
Viber	✗	✗
WhatsApp	✗	✗
Wickr Me	✓	✗
Wire	✓	✗

Mobile Contact Discovery

- Heavy tools: Multiparty Computation
- Private Set Intersection
  - Previously deemed too slow for smartphones
  - But: Smartphones get stronger and stronger!
  - Protocols get better!

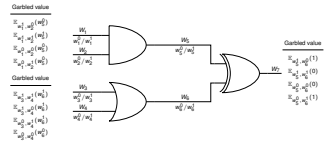
Results

D. Kales and C. Rechberger and M. Senker and T. Schneider and C. Weinert
Mobile Private Contact Discovery at Scale
USENIX Security Symposium 2019

https://contact-discovery.github.io/

https://ia.cr/2019/517

Results



- Multiple OPRF-based Protocols
  - Garbled Circuits using LowMC
  - Naor-Reingold
- Malicious Clients
- Implementation and Evaluation
  - Real smartphones (ARMv8 Cryptographic Extensions)
  - Fast online phase (2s for 1000 contacts over LTE)
  - Large one-time setup communication (1 GB for 2^{28} clients)

Wishes of large Messenging Services

- 1B+ monthly active users
- An address book with 10k users
- Latency: lookup time of < 2 seconds
- No large communication

Still a lot of improvement needed