Bundesministerium
Verkehr, Innovation
und Technologie

/informatik & security /fh/// st.pölten

Hochsichere, langzeitige Kryptografie für kabellose Kommunikation mit Integration von Funkmessdaten

Forschungsprojekt KIF

Projektleiter: Univ.-Doz. DI Dr. Ernst Piller

FFG
Forschung wirkt.

KIRAS
Sicherheitsforschung

Projektpartner

- FH St. Pölten (Institut für IT Sicherheitsforschung)
- Cryptas IT-Security GmbH: Wirtschaftspartner
- Bundesministerium für Europa, Integration und Äußeres (BMEIA): Bedarfsträger
- FH St. Pölten GmbH, Institut für Medienwirtschaft: GSK-Partner
- ASFINAG Autobahnen- und Schnellstraßenfinanzierungs-AG: LoI
- Bundesministerium für Landesverteidigung: LoI

Um was geht/ging es beim Projekt?

- Digitalisierung und Globalisierung benötigen sichere Kommunikation ➔ sichere Kommunikation benötigt Kryptografie ➔ Bedeutung der Kryptografie nimmt zu
- Projektschwerpunkte dabei: IoT, autonomes Fahren und Kommunikation über große Entfernungen
- Mathematische Verfahren der Kryptografie bauen auf Vermutungen auf, die nicht beweisbar sind ➔ Staaten (Geheimdienste) / Unternehmen haben evt. „Tools“ zum Knacken von verwendeter Kryptografie ➔
- **Physikalische Methoden der Kryptografie**

Erzeugung und Verteilung krypt. Schlüssel

- Verschlüsselung des Schlüssels oder Diffie-Hellman:
  - klassisch
  - elliptische Kurven
  - **Post-Quanten Kryptografie**
- Physikalisch:
  - persönlicher Transport: aufwendig, nicht massentauglich
  - Quantenkryptografie: teuer und nicht massentauglich
  - **Funkkanaleigenschaften**: Direktkommunikation (klassisch bis ca. 20km) und Satellitenkryptografie

Um was geht/ging es beim Projekt?

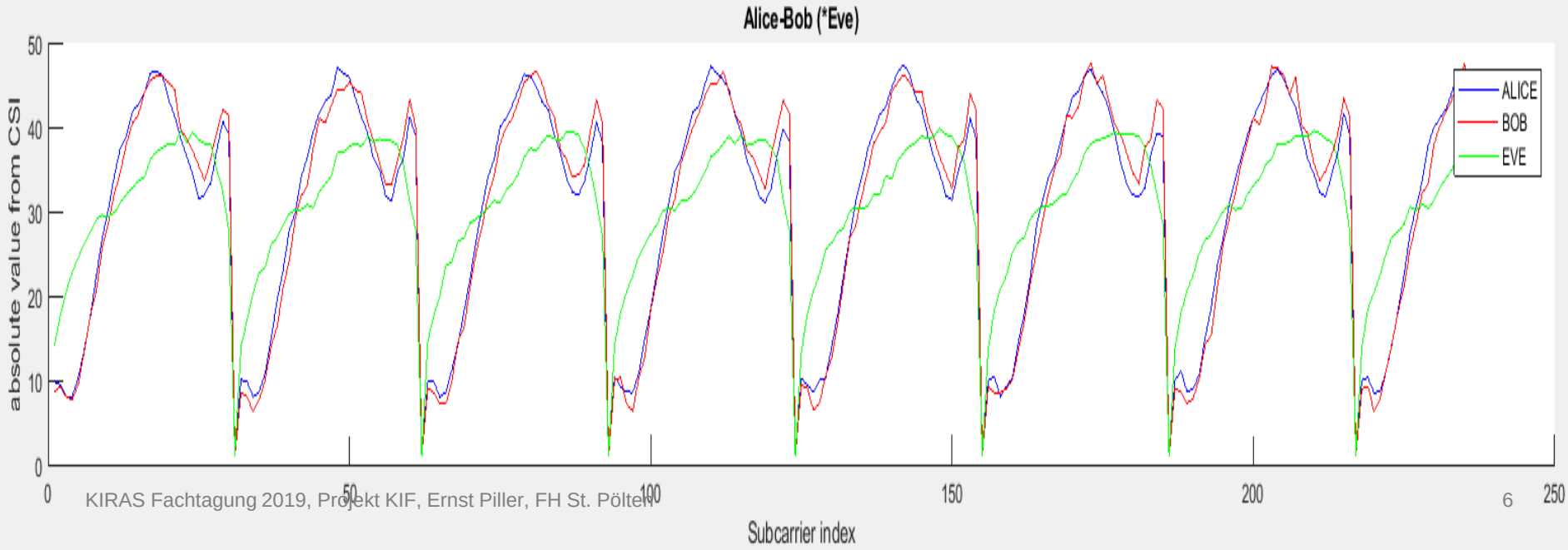
Lösung: Schlüsselerzeugung durch Messung von Funkkanaleigenschaften der Telekommunikation:

- Direkte Funk-Kommunikation (bis ca. 20km) gelöst, KIF hat die Geschwindigkeit wesentlich verbessert und eine hochsichere Authentifikation inkludiert
- Weltweite Funk-Kommunikation geht nur über Satelliten
  ➔ Satellitenkryptografie

Verbessern mathematische Methoden mit physikalischen Methoden und sind massentauglich einsetzbar

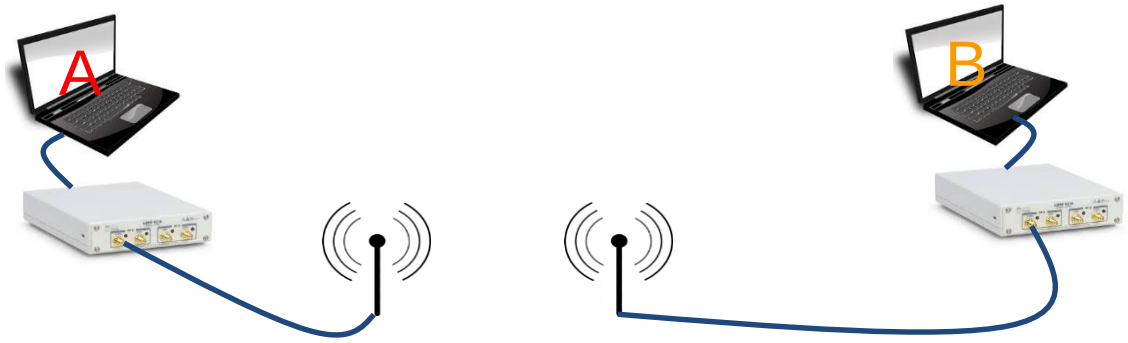
Funkkanaleigenschaften Direktkommunikation

- **Reziprozität**: bei Funkübertragung in beide Richtungen werden auf beiden Seiten identische Werte gemessen (Phasenwinkel, Signalstärke, …)
- **Dynamik erzeugen bewegte Objekte und Reflexionen**



Funkkanaleigenschaften im Projekt KIF

- Phasenwinkel statt Signalstärke: wesentlich genauer
- LSH abgeleitetes Verfahren zur Schlüsselberechnung
- Supersinguläre isogene elliptische Kurvenkryptografie (Post-Quanten-Kryptografie) für Authentifizierung der beiden Kommunikationspartner



Schlüsselberechnung-Verfahren

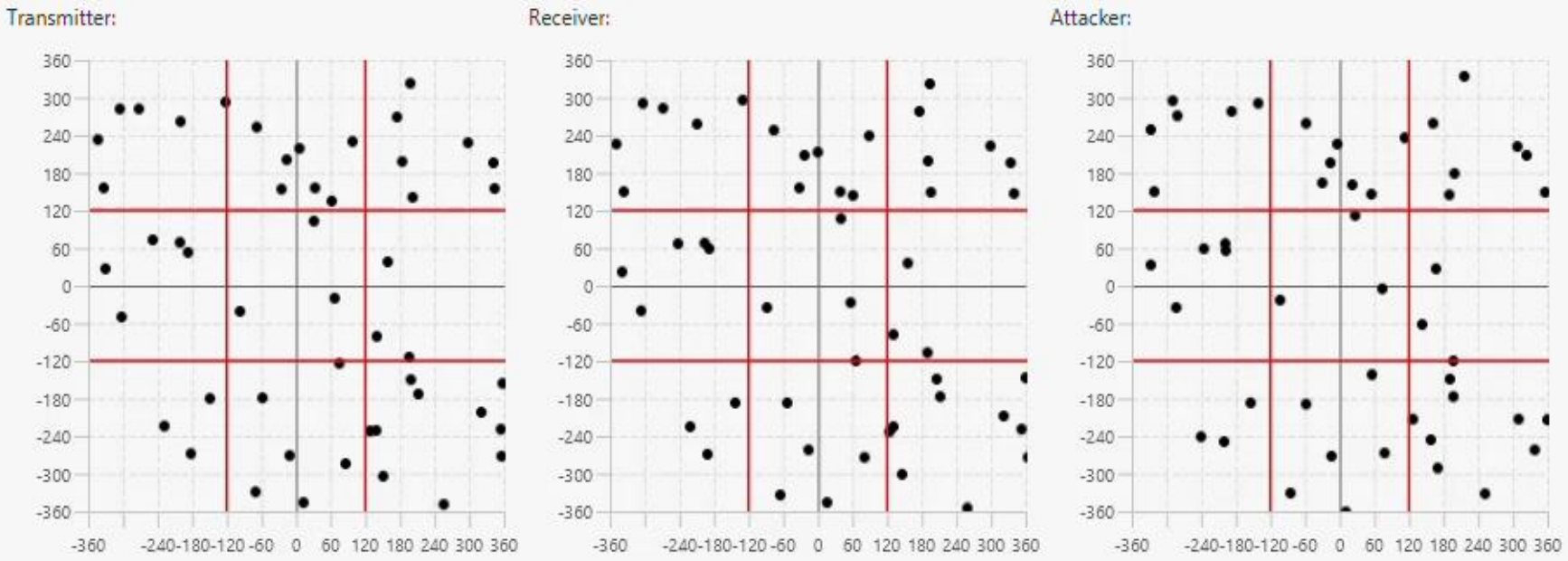
- Das Schlüsselberechnungsverfahren wurde von einem bekannten nearest-neighbour-search Verfahren, LSH (Locality Sensitive Hashing), abgeleitet
- Es enthält die verkettete Parametrisierung der physikalischen Eigenschaften (Messwerte) in einem n-dimensionalen Raum mit einer Teilung in Quadranten, um die Gleichverteilung nicht zu zerstören
- Ein Angreifer, der nicht alle physikalischen Gegebenheiten gleich hat und nur wenig abweicht, kann zu einer großen Wahrscheinlichkeit nicht denselben Schlüssel generieren

KIRAS Sicherheitsforschung

/informatik & security /fh/// st.pölten

Schlüsselberechnungs-Verfahren

(Abweichung Empfänger: 2,7 %, Abweichung Angreifer: 5,4 %)



Hash of Transmitter: dadb527cc95e99da6a05ad5ddc3b6e1529706761c1639a4df85ba8faad28305d

Hash of Receiver: dadb527cc95e99da6a05ad5ddc3b6e1529706761c1639a4df85ba8faad28305d

Hash of Attacker: 058e4eadabec23e9bb6648c6340bf81f7a4b8709aa4accf93fd1822fcdbcb6f6

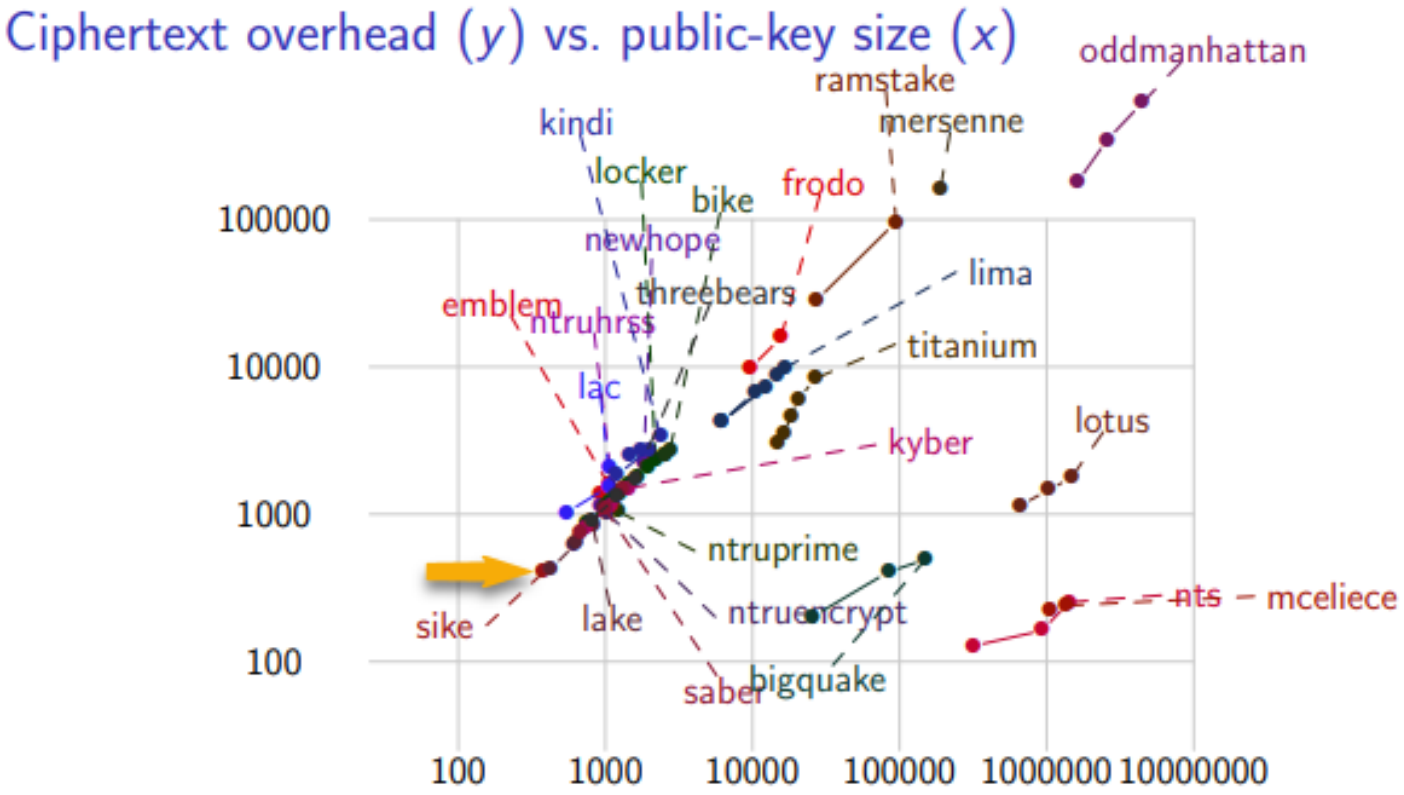
Supersinguläre isogene elliptische Kurven

- Basiert auf speziellen elliptischen Kurven und ist daher ähnlich zu bekannten Verfahren (ECDH, ECDSA)
  - das mathematische Problem ist aber anders
- Für kryptografische Anwendungen noch nicht so gut erforscht wie andere Post-Quanten-Verfahren
- Große Vorteile in der Schlüsselgröße, hier das bis jetzt effizienteste Verfahren
- Nachteile liegen noch in der Geschwindigkeit

Supersinguläre isogene elliptische Kurven

- Java-Version vollständig mit eigener Bibliothek entwickelt ➔ **fertig implementiert und optimiert**
- Geschwindigkeit optimiert / verbessert, sie bietet aber noch weitere Verbesserungsmöglichkeiten. Schlüssel-Enkapsulierungsmethode auch vollständig vorhanden
- Unsere Software kann sehr einfach in vorhandene Software integriert (implementiert) werden, weil sehr modular aufgebaut ➔ **empfehlenswert für alle neuen Software-Produkte mit Kryptografie**

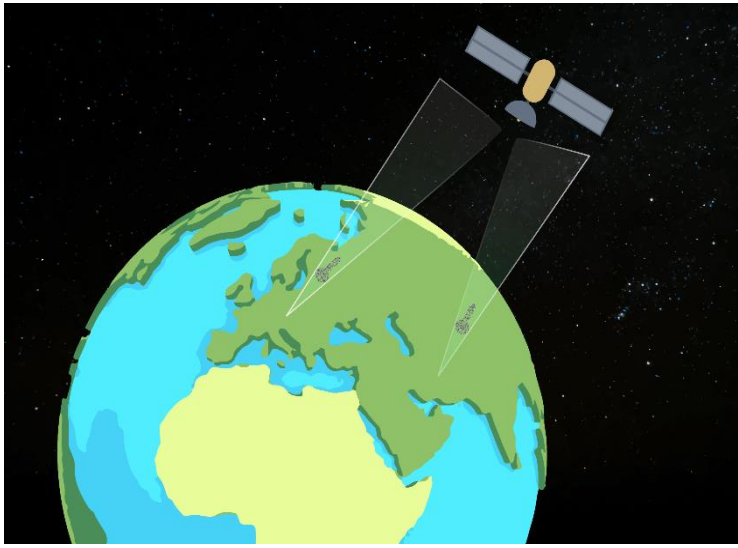
NIST – Round 1


Ciphertext overhead (y) vs. public-key size (x)
oddmanhattan
ramstake
kindi
mersenne
locker
bike
frodo
100000
newhope
lima
threebears
emblem
ntruhrss
titanium
10000
lac
lotus
kyber
1000
ntruprime
sike
lake
ntruencrypt
nts
mceliece
100
saber
bigquake
100
1000
10000
100000
1000000
10000000

Satellitenkryptografie

Unterschiede zur Direktkommunikation:

- Satelliten erforderlich, die idealen man-in-the-middle darstellen, d.h. alle Daten an alle weitersenden
- Satelliten liefern aber auf Grund ihrer hohen Umlaufgeschwindigkeit hohe Dynamik
- Umwelteinflüsse (Brechungen etc.) beeinflussen Messergebnisse (sind reziprok, daher verwendbar)



Satellitenkryptografie

Lösung:

Post-Quanten-Kryptografie, Ausnützung der Geschwindigkeit und Ungenauigkeit der Umlaufbahnen, Spread Spectrum, Ausnützung Umwelteinflüsse, …..

Schlüsselberechnung ähnlich wie bei Direktkommunikation, aber mit großen neuen Herausforderungen

Weltweit komplett neu, keine einzige Publikation und kein Patent - wir haben erstes Patent angemeldet

Folgeprojekt geplant

Danke für Ihre Aufmerksamkeit!