UNIVERSITÄT DES SAARLANDES

hgi Horst Görtz Institut für IT-Sicherheit

RUHR UNIVERSITÄT BOCHUM

RUB

Zero-Communication Seed Establishment for Anti-Jamming Techniques

Kim Pecina and **Esfandiar Mohammadi**
(CISPA / Saarland University, Germany),
Christina Pöpper
(HGI / Ruhr-University Bochum, Germany)

Feb 23rd, 2014

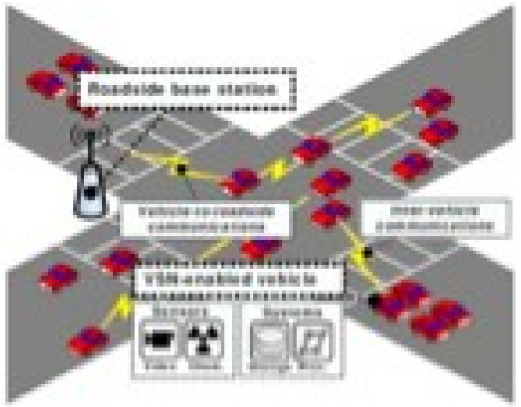
Wireless Communication

Wireless communication is applied in more and more domains for monitoring, support, and control

- Industry and industrial infrastructure
- Critical infrastructure
- Vehicle/traffic communication

© http://novotek-tankfarm.ru

©http://airliquide.at



Vehicular Networks (VANETs)

Jamming Attacks

DoS-attack, part of more sophisticated attacks

Jamming devices are easy/cheap to obtain

- starting at ~ 100$

Common countermeasure:

- Evade the jammer by using spread-spectrum techniques (FH, DSSS)
- Common anti-jamming techniques rely on pre-shared secret codes (output of a seeded/keyed PRNG)

Setting up Shared Secret Keys

Key Pre-Loading

- Clean solution whenever applicable
- Pre-loading the keys suffers from distribution, revocation, and scalability problems

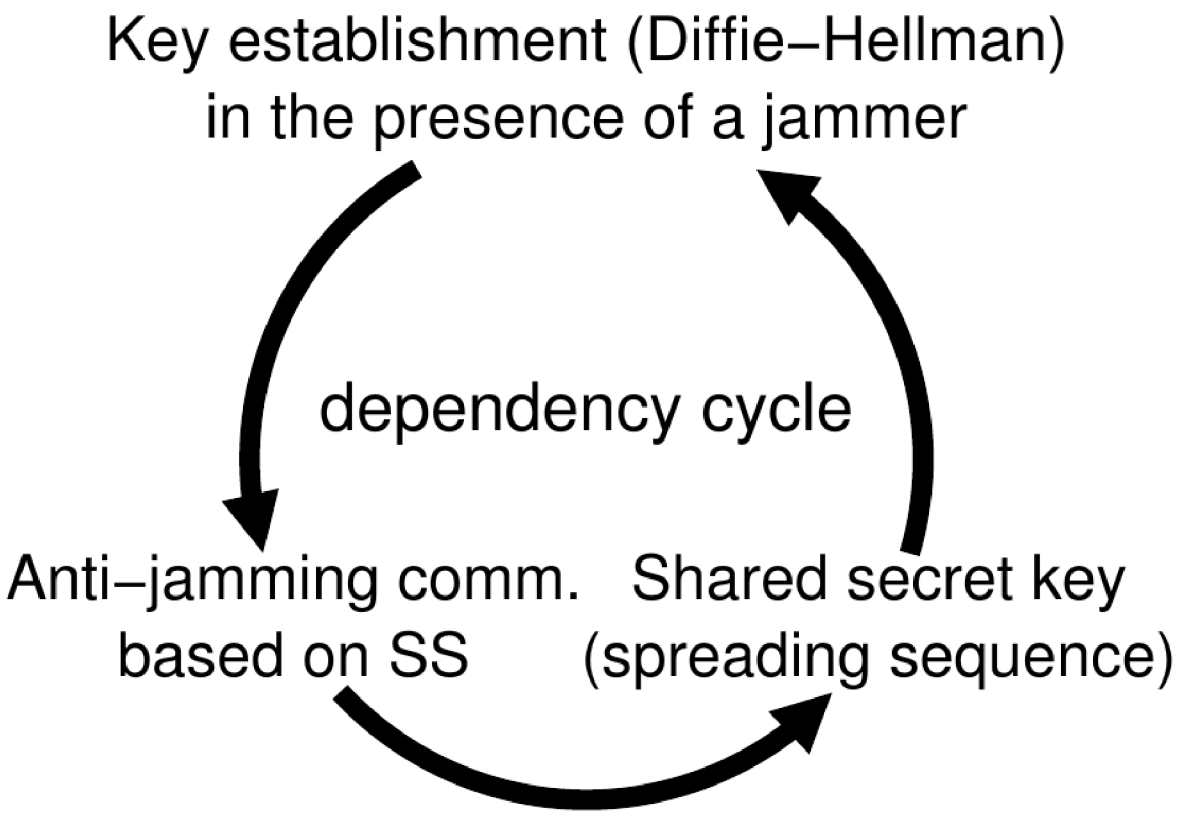
Ad-hoc Key Establishment

- Key-establishment protocols using public key cryptography solve most of these problems
- But they assume the existance of jamming-resilient communication

  ⇝ Devices need to communicate to establish shared keys

Key Establishment in the Presence of Jammers

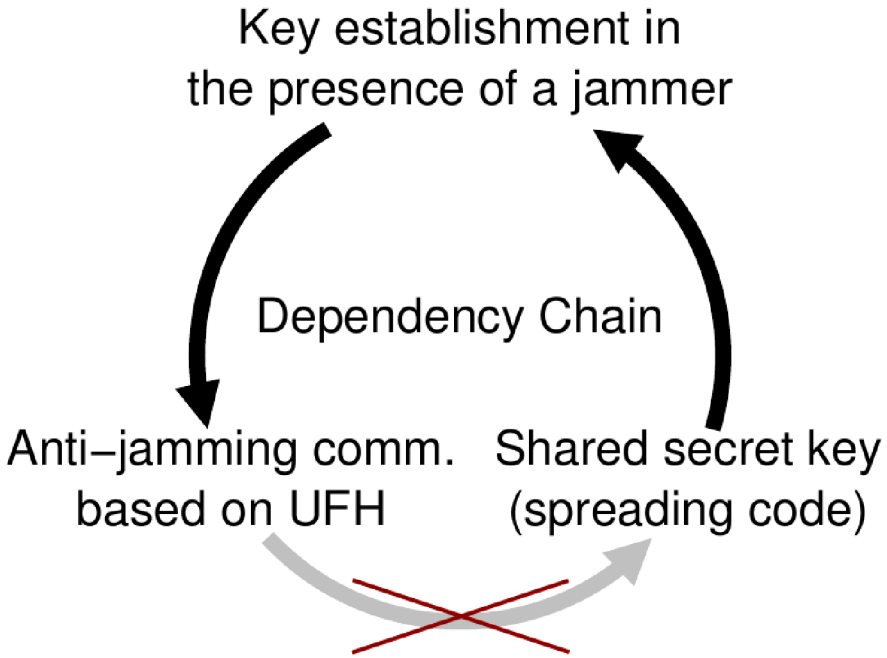
Anti-Jamming Key-Establishment Dependency [26]



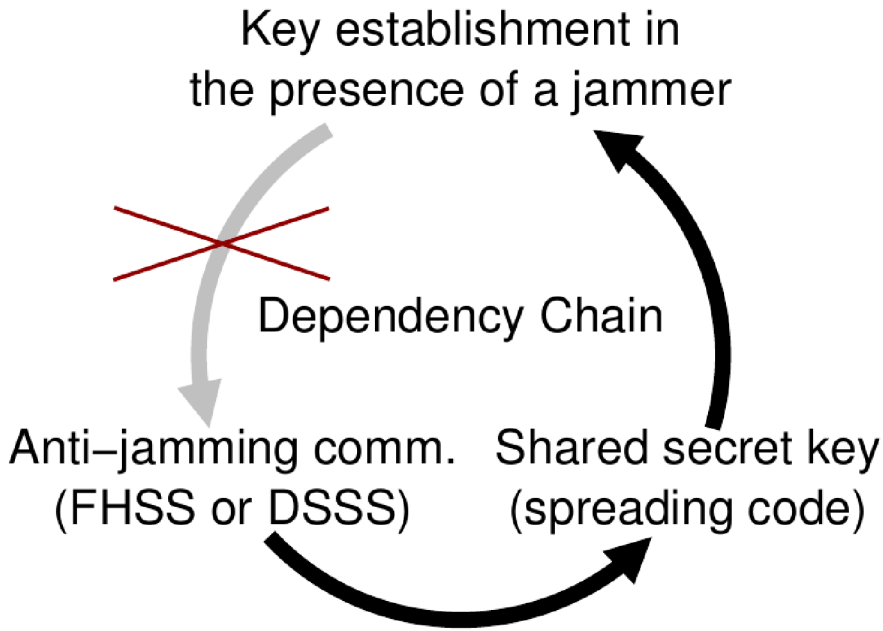
[26] Strasser et al.: Jamming-resistant key establishment using Uncoordinated Frequency Hopping. IEEE Symposium on Security and Privacy (S&P), 2008.

Key Establishment in the Presence of Jammers

- Communication-based solutions (using PKC):
  - UFH [25,26], UDSSS [19], RD-DSSS [15], DSD-DSSS [14], ZPK-DSSS [10], ...



- Solutions using ID-based cryptography:
  - This work
  - [3]

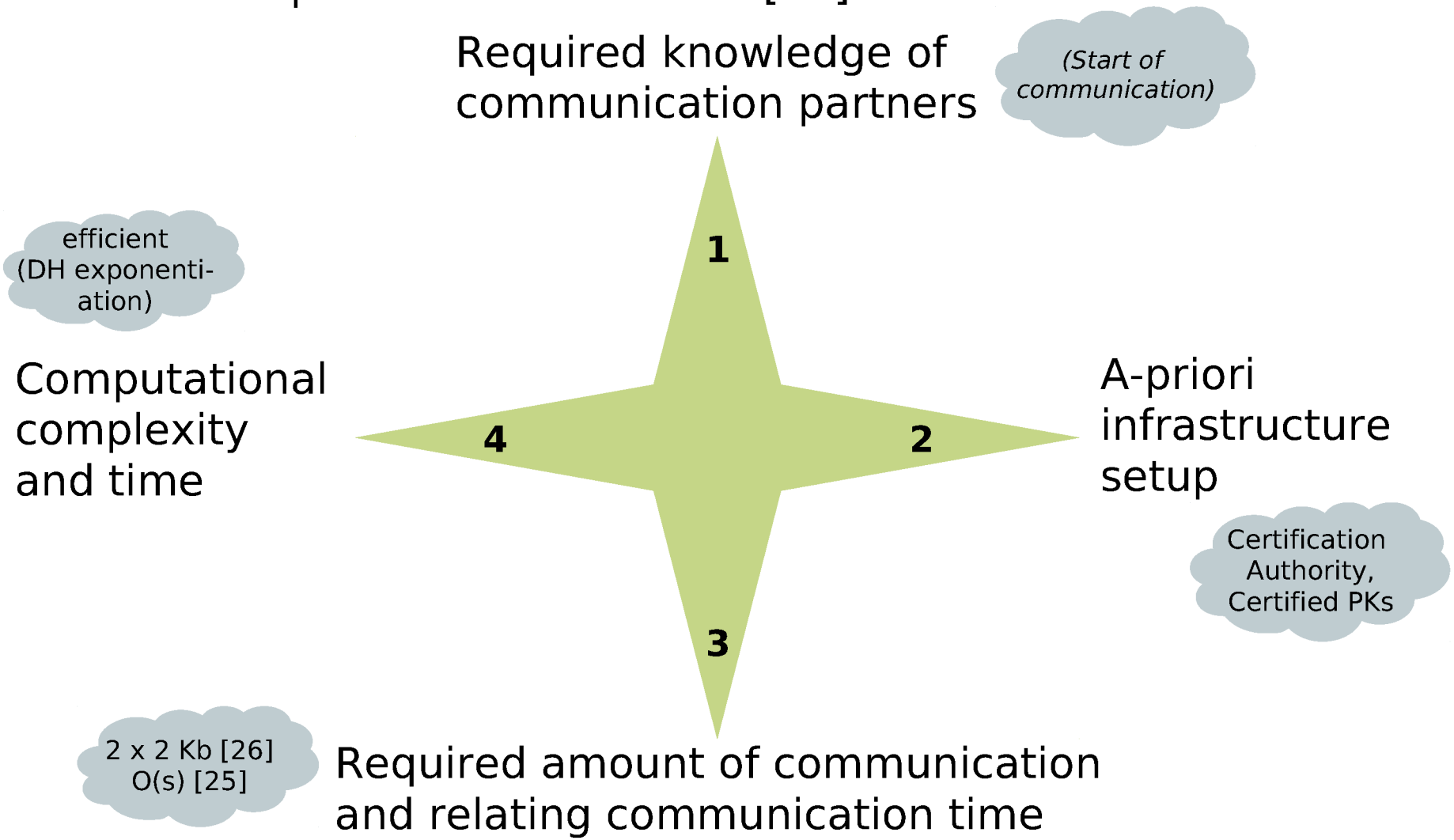


[3] Capar, Goeckel, Paterson et al.: Signal-flow based analysis of wireless security protocols. Information and Computation, 2013.

Solution Space

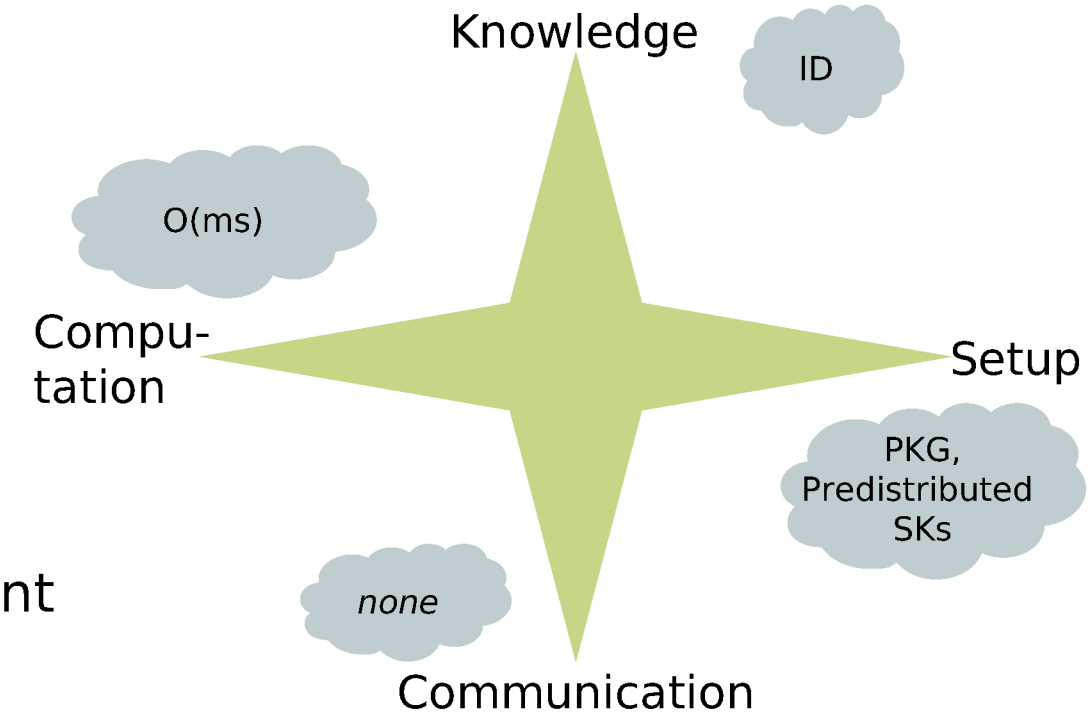
Dimensions of the solution space:

- on the example of PKC-based UFH [26]



Our Proposal

- Use identity-based cryptography
  - Public key is derived from the communication partner´s ID (public, long term, rather short)
  - E.g., email address, MAC address, license plate number
  - Overcome static nature of the established keys by using time information
- Prerequisite
  - Trusted central private key generator (PKG)
  - IDs are known / can be obtained visually
- Result
  - Efficient seed establishment without communication



ID-based Approach

Setup phase (before the start of AJ communication)

- Public key = hash of the ID, mapping strings to group elements (on an elliptic curve)
  - $\mathrm{pk}_A := h(\mathrm{ID}_A) = a \cdot g$, i.e., $a := \mathrm{dlog}_g(\mathrm{pk}_A)$
- The (trusted) private key generator generates for all parties their private keys (using a master secret s):
  - $\mathrm{sk}_A := s \cdot \mathrm{pk}_A = sa \cdot g$

Key generation for subsequent AJ communication (basic idea):

- $e(\mathrm{sk}_A, \mathrm{pk}_B) = e(as \cdot g, b \cdot g) = e(g,g)^{abs} = e(\mathrm{sk}_B, \mathrm{pk}_A)$ where $e(\cdot,\cdot)$ is the bilinear pairing $e : \mathbb{G}_1 \times \mathbb{G}_1 \to \mathbb{G}_T$ for two groups
- For providing unpredictability, we add the current time frame: $\mathcal{S}_{(A,B)} := f(e(\mathrm{sk}_A, \mathrm{pk}_B), tf) = f(e(g,g)^{abs}, tf)$

Further Contents

Cryptographic security analysis

- Security notion based on the eCK model [13] for a (mutually authenticated) secure key
- Proof that the established seed is pseudo-random (in the random oracle model)
  - Adversary can request the challenge and compromise parties
- Definition of a Pseudo Random Seed Challenger $\mathrm{PRSCh}_b(1^\eta)$ against the pseudo-randomness of the seed establishment
  - Adjusted to a setting with timeframes
  - Worst case assumption: adversary can decide when a new timeframe begins

[13] LaMacchia, Lauter, and Mityagin, “Stronger security of authenticated key exchange,” in Proceedings of the International conference on Provable Security, ProvSec. 2007

Implementation Details

- Implementation in Java
  - Java API for hash function (SHA-256) and standard ms time
- Cryptographic operations
  - jPBC library [4], released under the LGPL v3 licence
- Elliptic curves
  - Symmetric TYPE-I (Type-A), embedding degree k = 2
  - Security parameter η bit, bit sizes r = 2η ($\mathbb{G}_1$), p (elliptic curve base field)

RSA	η	r	p	$\lvert\mathbb{F}_{q^2}\rvert$
1024	80	160	512	1024
2048	112	229	1099	2198
3072	128	260	1599	3198

Recommendations [12]

- Source code and executables are available at `http://sps.cs.uni-saarland.de/zcaj`:
  - Android APK & Jar file

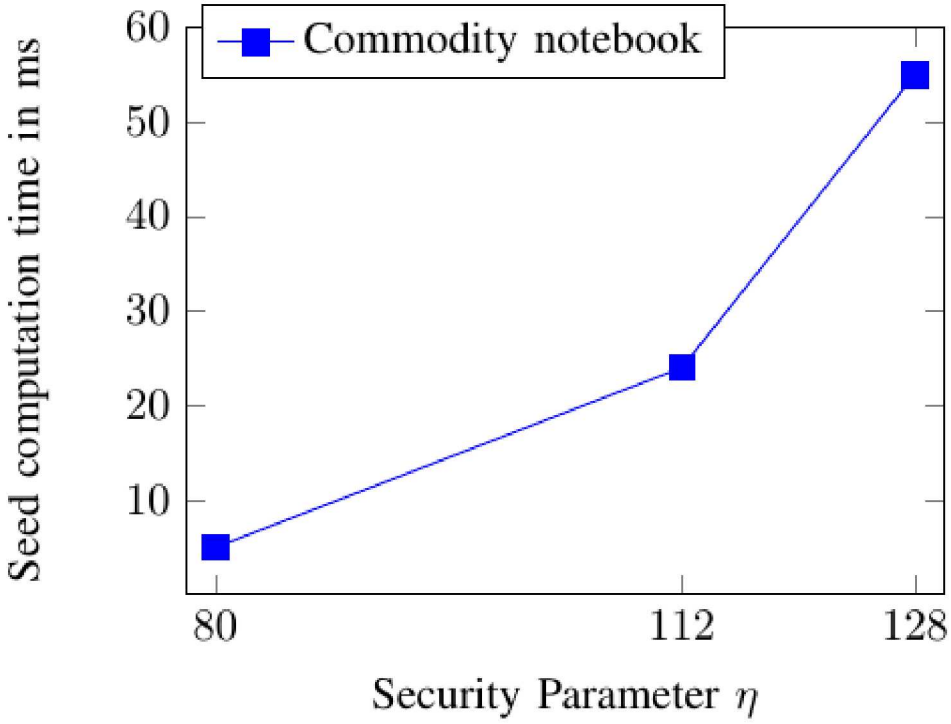
[4] De Caro and Iovino: jPBC: Java pairing based cryptography. In Proceedings of ISCC, 2011, http://libeccio.dia.unisa.it/projects/jpbc/download.html

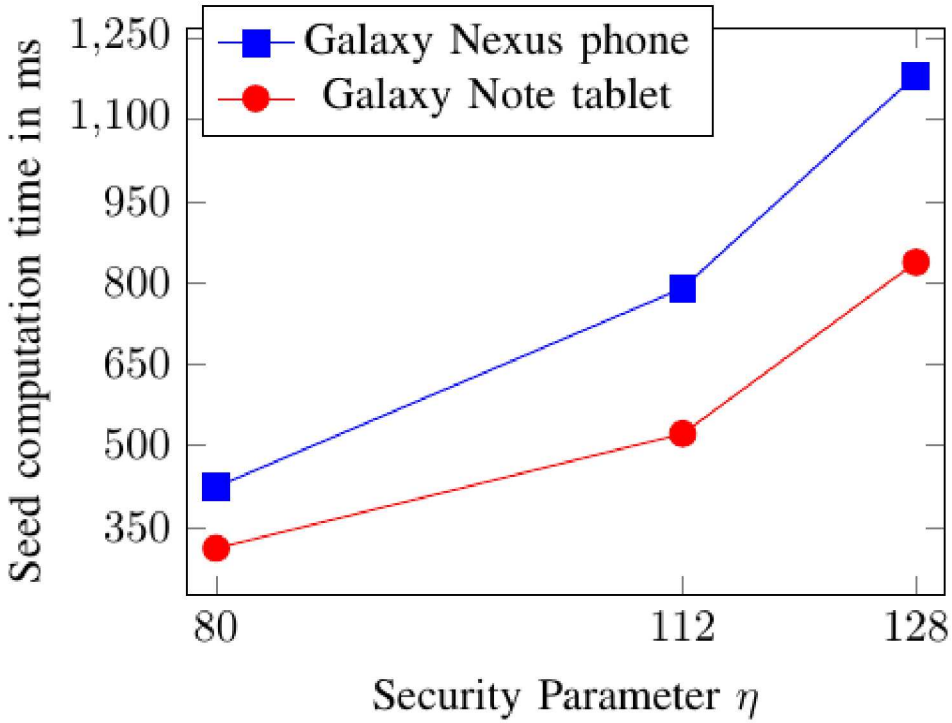
[12] Koblitz and Menezes, “Pairing-based Cryptography at High Security Levels”, 2005.

Implementation Results

3.3 GHz quad-core

1.2 GHz dual-core & 1.4 GHz quad-core





Application of the ID-based Approach

Application

- When IDs are known / can be obtained, but the set of potential partners is too large to store shared keys for each
  - Often communication does not happen with random parties

- When IDs are not known, they must be authentically obtained using AJ communication
  - Whenever IDs are shorter than public keys, the ID-based approach can still provide benefits (shorter messages) [3]

© http://novotek-tankfarm.ru

Conclusion and Open Questions

- Securing wireless communication is crucial for numerous applications
  - Industrial communication, infrastructure-critical communication, smart grids, etc.
- Jamming attacks are serious threats and hard to counter

- We investigated the use of **ID-based cryptography for anti-jamming key establishment**

- Open problem:
  - How to generally identify the desire for AJ communication (w/o visual channels or scheduled transmissions): When? Who?

Thank you for your attention

pecina@cs.uni-saarland.de mohammadi@cs.uni-saarland.de christina.poepper@rub.de