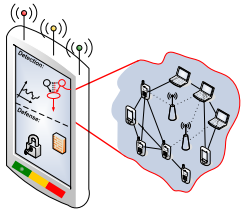


SKIMS
A Cooperative Autonomous Immune System
for Mobile Devices

Hochschule für Angewandte Wissenschaften Hamburg
Hamburg University of Applied Sciences

Angriffe auf Funknetzwerke

Heiner Perrey

Betreuer: Dirk Westhoff

Anwendungen 2,
01. Juni 2011

Overview

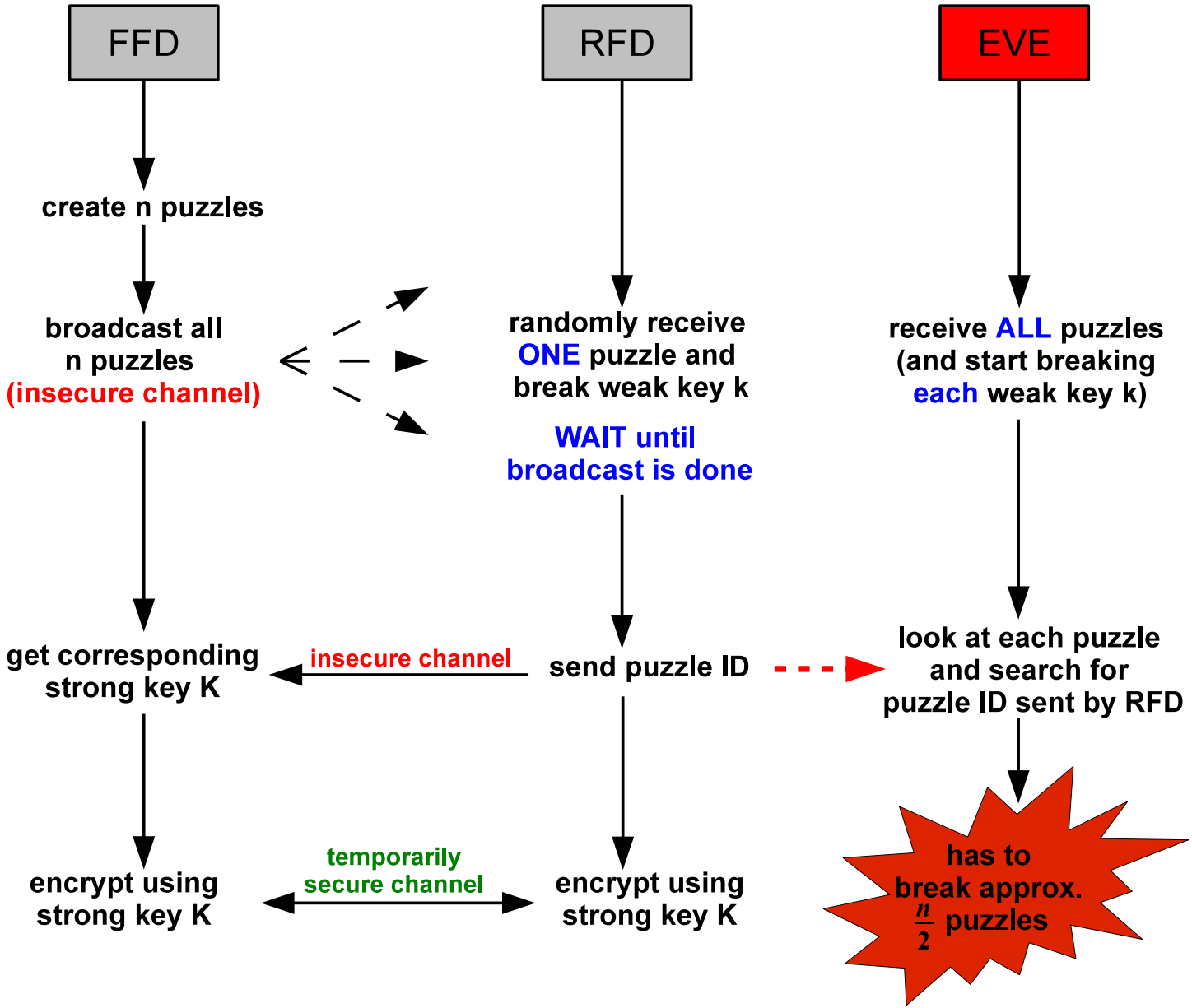
AW1: Problemstellung

- Schlüsselaustausch zwischen einem leistungsstarken und mehreren leistungsschwachen Geräten per Bluetooth Low Energy (BLE)
- Leistungsschwache Geräte können keine komplexen Schlüsselaustauschverfahren einsetzen.
- BLE bietet zur Zeit keinen Schutz gegen passive Angriffe.

AW1: Lösungsweg

- Nutzung des Merkle's Puzzle (MP) für den Schlüsselaustausch
- Das leistungsstarke Gerät übernimmt die Rechenlast für beide.
- Hierfür soll MP in die Bluetooth Spezifikation mit aufgenommen werden.

Merkle's Puzzle



Content

Veröffentlichung der Gruppe Armknecht (2009)

- Arbeitsgruppe:
  - Frederik Armknecht: Junior Professor an der Ruhr-Universität Bochum im Bereich *IT-Sicherheit*
  - Dirk Westhoff: Professor an der HAW Hamburg im Bereich *IT-Sicherheit*
- Paper: „Using Merkle's Puzzle for Key agreement with Low-end Devices“ [2]:
  - Schlüsselaustausch zwischen Geräten mit asymmetrischen Kapazitäten durch Merkle's Puzzle
  - Motivation für dieses Paper: *Grundlage für meine Arbeit*

Armknecht et al. (2009): [2]

- Schlüsselaustausch zwischen einem leistungsstarken und einem oder mehreren leistungsschwachen Geräten
- Nutzung von Merkle's Puzzle, um Rechenlast auf das leistungsstärkere Gerät zu schieben
- Bezug auf *Wireless Body Area Networks* (WBAN) mit Zigbee.

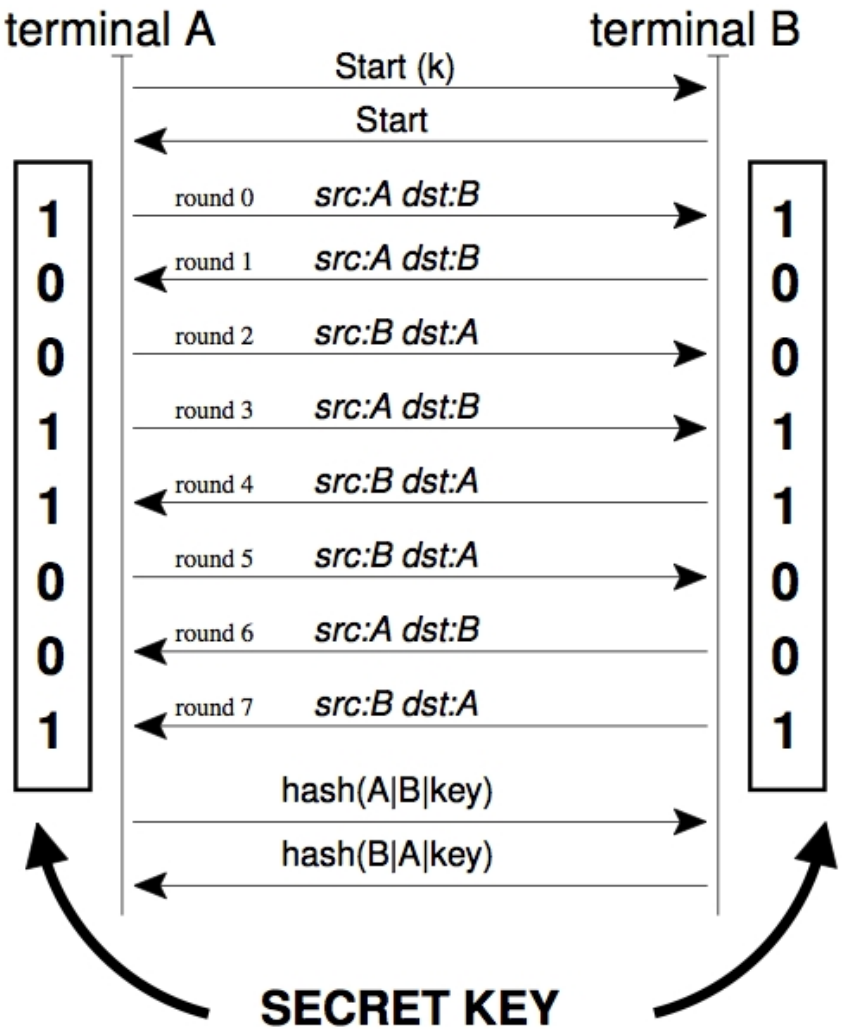
Armknecht et al. (2009): [2]

- Ggf. auftretende Schwierigkeiten:
  - relativ langwieriges Verfahren (Schlüsselaustausch kann mehrere Stunden dauern)
  - Sicherheit nur temporär und unter statistischer Annahme getroffen (theoretisch kann Angreifer sofort Erfolg haben)

Veröffentlichung der Gruppe Castelluccia (2005)

- Projekt
  - INRIA: National Institute for Research in Computer Science and Control [5]
- Arbeitsgruppe:
  - Claude Castelluccia: Senior Research Scientist bei INRIA
  - Pars Mutaf: Mitarbeiter bei INRIA
- Paper: „Shake Them Up!“ [4]:
  - Prävention eines Lauschers durch Schütteln der Geräte
  - Motivation für dieses Paper: *Kreativer Ansatz, der beschränkte Kapazitäten der Geräte mitberücksichtigt*

Castelluccia (2005): „Shake Them Up!“ [4]



Key exchange with „Shake Them Up“ [4]

- Verfahren:
  - Kommunikation über einen *anonymen Kanal* [1].
  - *A* und *B* senden mit variabler Quell- und Ziel-ID:
    - ★ IDs sind korrekt: Key-Bit $= 1$
    - ★ IDs sind falsch: Key-Bit $= 0$
  - Lauscher weiß nicht, ob IDs korrekt sind
  - Schütteln der Geräte, um z.B. *Signalstärke-Analyse* zu verhindern

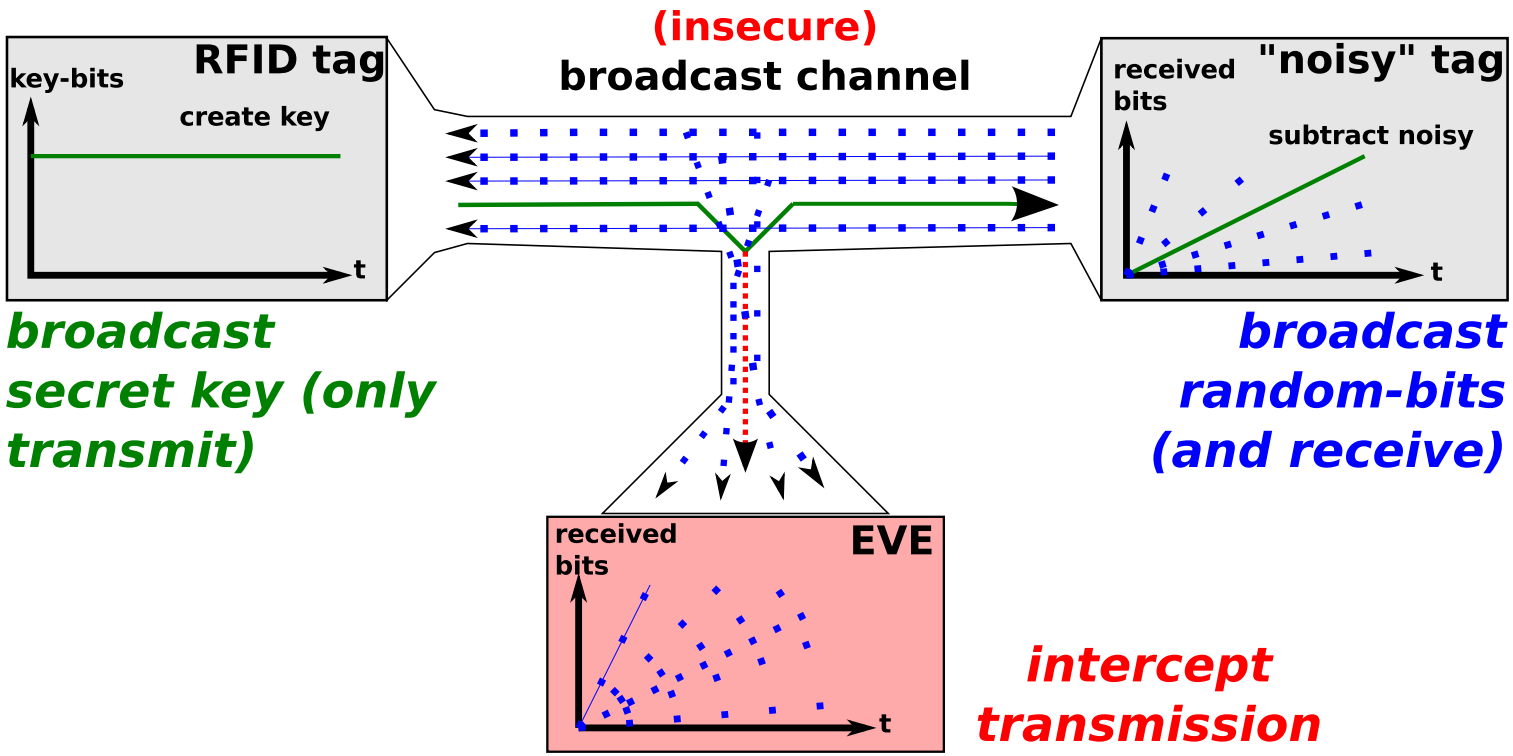
Castelluccia (2005): „Shake Them Up!“ [4]

- Ggf. auftretende Schwierigkeiten:
  - erfordert User-Input (Schütteln der Geräte)
  - Einsatz in Bluetooth ist nicht möglich, da anhand *time devision multiplexing access* (TDMA) Quelle identifizierbar ist.
  - benötigt einen (halbwegs) zuverlässigen Kanal

Veröffentlichung der Gruppe Castelluccia (2006)

- Projekt
  - INRIA: National Institute for Research in Computer Science and Control [5]
- Arbeitsgruppe:
  - Claude Castelluccia: Senior Research Scientist bei INRIA
  - Gildas Avoine: Professor an der UCL in Belgien (damals Doktorand an der *Eidgenössischen Technischen Hochschule Lausanne* (EPFL))
- Paper: „Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags“ [3]:
  - Prävention eines Lauschers durch Überfluten des Mediums mit Rauschen
  - Motivation für dieses Paper: *Kreativer Ansatz, der beschränkte Kapazitäten der Geräte mitberücksichtigt*

Castelluccia (2006): „Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags“ [3]



Key exchange between RFID- & Noisy-tag.

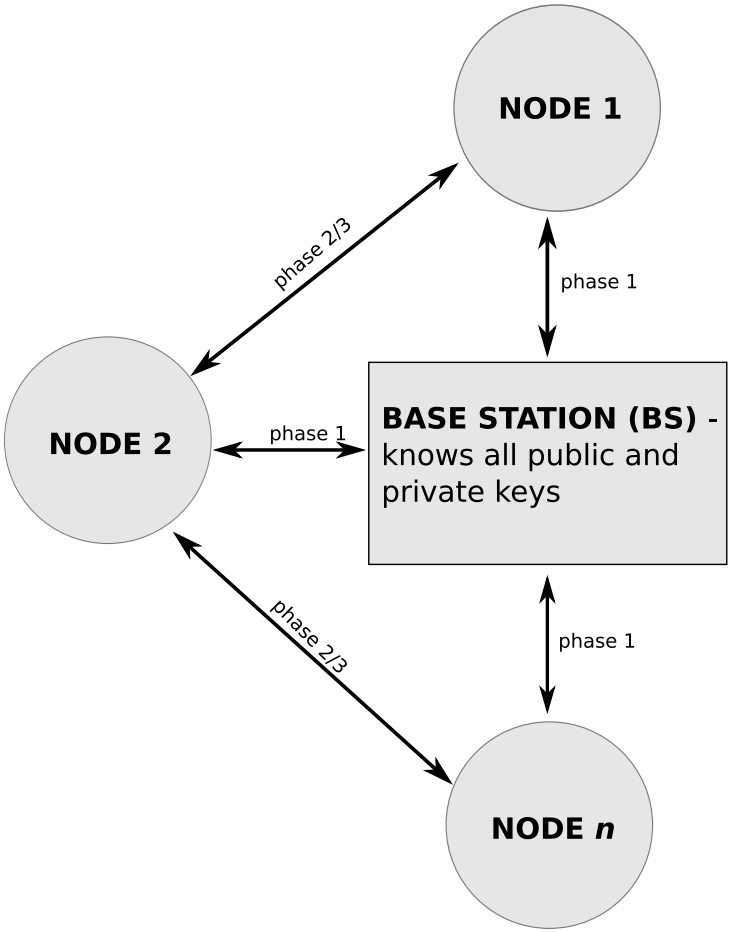
Castelluccia (2006): „Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags“ [3]

- Ggf. auftretende Schwierigkeiten:
  - Quelle darf nicht identifizierbar sein.
  - benötigt einen zuverlässigen Kanal und zeitliche Synchronisation

Veröffentlichung der Gruppe Salam (2010) [8]

- Die Arbeitsgruppe:
  - I. Salam: Student der Dongseo University (Süd Korea)
  - HoonJae Lee: Prof. an der Dongseo University
  - P. Kumar: Doktorand von HoonJae Lee
- Paper: „An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography“ [8]:
  - Bootstrapping Problem: Schlüsselaustausch durch asymmetrische Verfahren
  - Motivation für dieses Paper: *Standard-Ansatz (Kombination symmetrischer und asymmetrischer Kryptographie, für WSN optimiert)*

Salam (2010): „An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography“ [8]



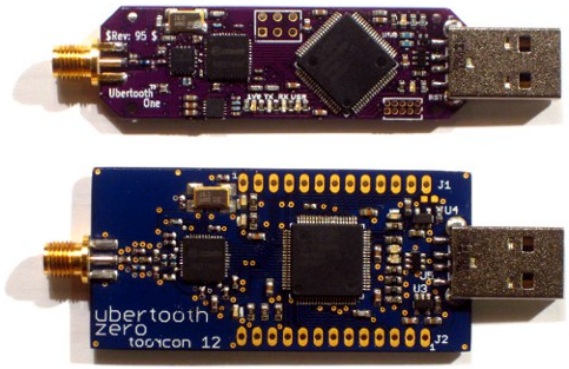
Key exchange using pre-distribution scheme

- Optimierung für WSN:
  - Jeder Knoten kennt nur seine direkte Nachbarn (weniger Schlüssel im Speicher)
  - symmetrischer Key zur weiteren Optimierung
- Vorschlag: ein 3-Phasen-Modell, das auf Public-Private-Key-Kryptographie basiert

Salam (2010): „An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography“ [8]

- Ggf. auftretende Schwierigkeiten:
  - Public-Private-Key-Verfahren sind relativ aufwendig (mind. einmal muss asym. Verfahren genutzt werden).
  - Durch Basis-Station ist eine Art *vertrauenswürdige Einheit* nötig.
- In einem Review-Paper wird auf einige dieser Schwierigkeiten eingegangen [9].

Arbeit von Michael Ossmann [6, 7]



Ubertooth Zero & One [7]

- Entwickelt Bluetooth Monitoring-Geräte: *Ubertooth Zero* & *One*.
- Sniffing Tools für Bluetooth etwas aufwendiger als z.B. für WLAN.
- Entwicklung eines BLE-Monitoring-Gerätes
- Sensibilisierung für Sicherheitslücken

Content

Abgrenzung: Armknecht et al.

- In meiner Arbeit soll die gleiche Idee für BLE als neue Technologie weitergeführt werden.
- Ggf. Untersuchung anderer Bereiche (z.B. praktische Umsetzung).
- Durch die höhere Übertragungsrate von BLE kann das Verfahren optimiert werden.

Abgrenzung: Castelluccia et al.

- Vermeidung von User-Input oder zusätzlicher Hardware für den automatisierten Schlüsselaustausch
- durch *time devision multiplexing access* (TDMA) in BLE nicht nutzbar (entlarven der Quelle möglich)
- benötigt einen (halbwegs) zuverlässigen Kanal und zeitliche Synchronisation

Abgrenzung: Salam et al.

- Auf klassische Public-Private-Key-Verfahren soll verzichtet werden.
- Eine *vertrauenswürdige Einheit* soll nicht eingesetzt werden.

Abgrenzung: Ossmann

- bietet Grundlage für meine Arbeit: ohne Sniffing-Tool kein Lauschen möglich
- Meine Arbeit versucht, einen so durchgeführten Angriff abzuwenden.

Content

Zusammenfassung

- Masterprojekt:
  - Schlüsselaustausch für Geräte mit asymmetrischen Kapazitäten.
  - Nutzung des Merkle's Puzzle, um schwache Geräte zu entlasten und Schlüsselaustausch zu ermöglichen
- Vorgestellte verwandte Arbeiten:
  - Standard-Ansätze (asymmetrische- und symmetrische Kryptographie) [8]
  - kreative Ansätze (z.B. Schütteln der Geräte) [3, 4]
  - „Eigeninitiative“ [6, 7]

[1] B. Alpern and F. Schneider.
Key Exchange Using “Keyless Cryptography”.
inf. Process. Lett., pages 79–81, 1983.

[2] F. Armknecht and D. Westhoff.
Using Merkle’s Puzzle for Key agreement with Low-end Devices.
IEEE 34th Conference on Local Computer Networks, 2009. LCN 2009., pages 858–864, December 2009.

[3] G. Avoine and C. Castelluccia.
Noisy Tags: A Pretty Good Key Exchange Protocol for RFID Tags.
Smart Card Research and Advanced Applications, 7th IFIP WG 8.8/11.2 International Conference, pages 289–299, April 2006.

[4] C. Castelluccia and P. Mutaf.
Shake them up! A movement-based pairing protocol for CPU-constrained devices.
Proceedings of the 3rd international conference on Mobile systems, applications, and services, pages 51–64, December 2005.

[5] Wikipedia: INRIA.
webpage.
http://en.wikipedia.org/wiki/National_Institute_for_Research_in_Computer_Science_and_Control - last checked: 21.05.2011.

[6] mossmann's blog.
webpage.
http://ossmann.blogspot.com/ - last checked: 13.05.2011.

[7] Project Ubertooth.
webpage.
http://ubertooth.sourceforge.net/ - last checked: 20.05.2011.

[8] I. Salam, P. Kumar, and HoonJae Lee.
An Efficient Key Pre-distribution Scheme for Wireless Sensor Network Using Public Key Cryptography.

Sixth International Conference on Networked Computing and Advanced Information Management (NCM), 2010, pages 402 – 407, August 2010.

[9] I. Salam and HoonJae Lee.
A review on the PKC-based security architecture for wireless sensor networks.
In *2010 5th International Conference on Computer Sciences and Convergence Information Technology (ICCIT)*, pages 649 –652, December 2010.