Building Femtocell More Secure with Improved Proxy Signature

Chan-Kyu Han, Hyoung-Kee Choi, In-Hwan Kim

Sungkyunkwan University

IEEE GLOBECOM 2009, Honolulu, Hawaii, USA

CISS-07: Wireless Network Security

3 December, 2009

SUNG KYUN KWAN UNIVERSITY

School of Information and Communication Engineering

Computer Engineering

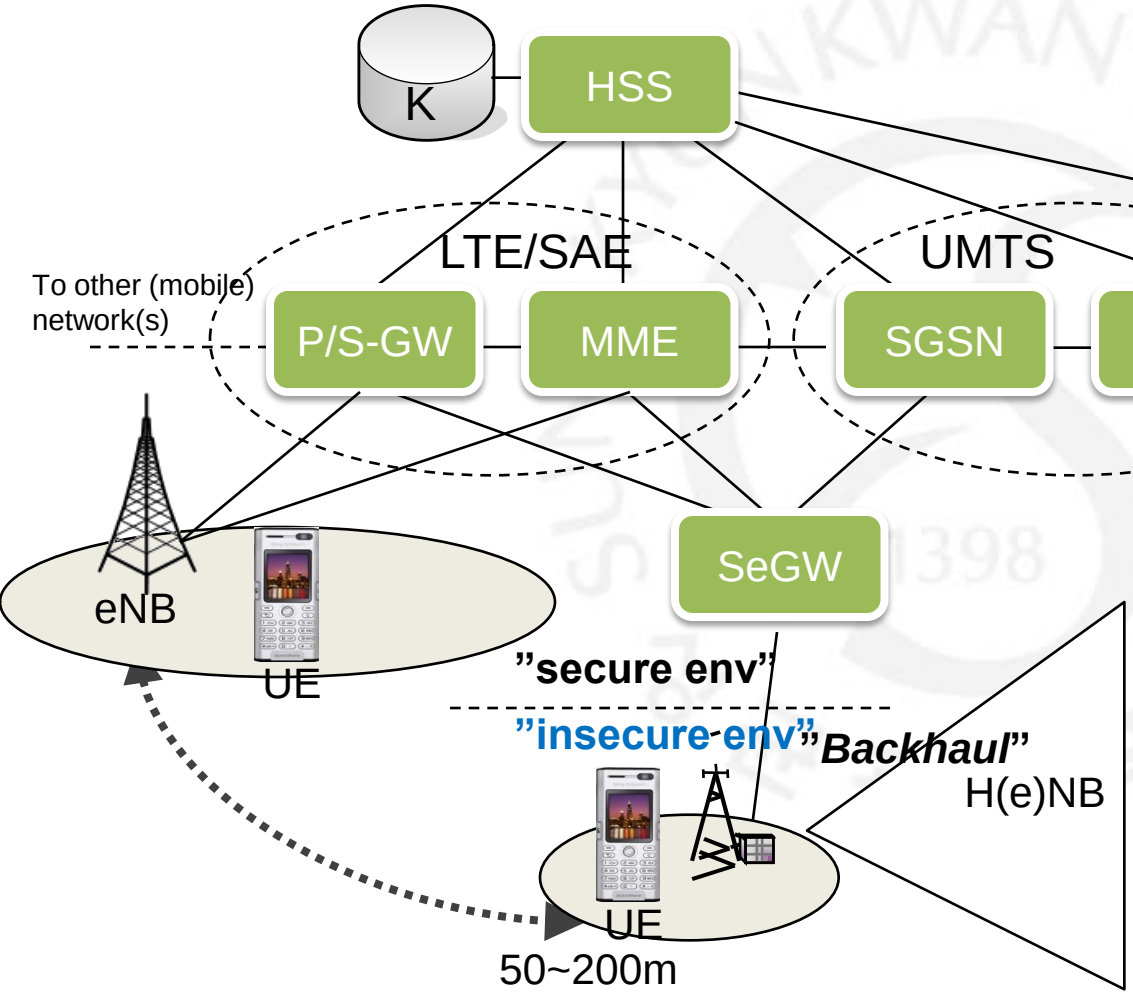
In a Nutshell

- Introducing the femtocell architecture in 3GPP
- Presenting security weaknesses of femtocell
- Proposing an enhanced proxy signature scheme to build femtocell more secure
- Analyzing security and performance of proposed scheme

FEMTOCELL

- Mini base station for home and office
- Operates in the licensed spectrum
- Connects via broadband Internet

3GPP HeNB/HNB ARCHITECTURE

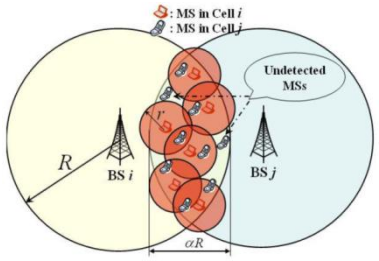


HIT

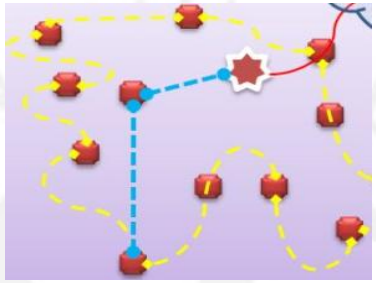
SUNG KYUN KWAN UNIVERSITY

MOTIVATION

Deployment



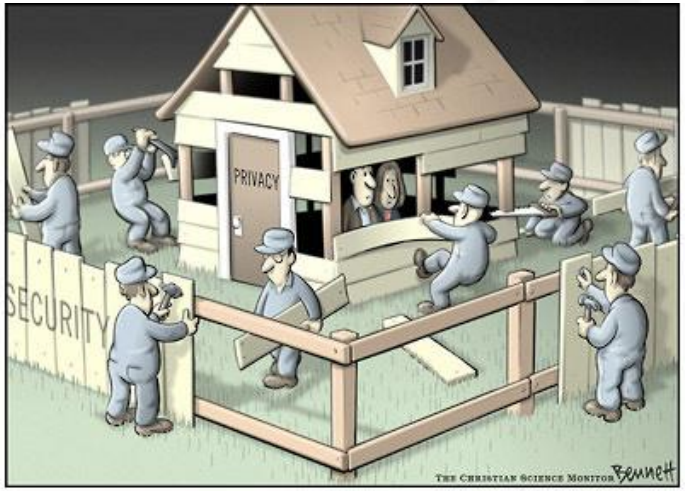
Interference



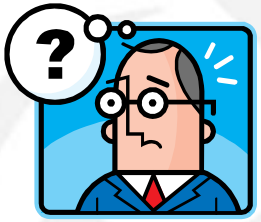
Self-organization

Handover

Emergency calls



Security and Privacy



NEC's Femtocell Serivices :
Femtocell as a Home Security Enabler

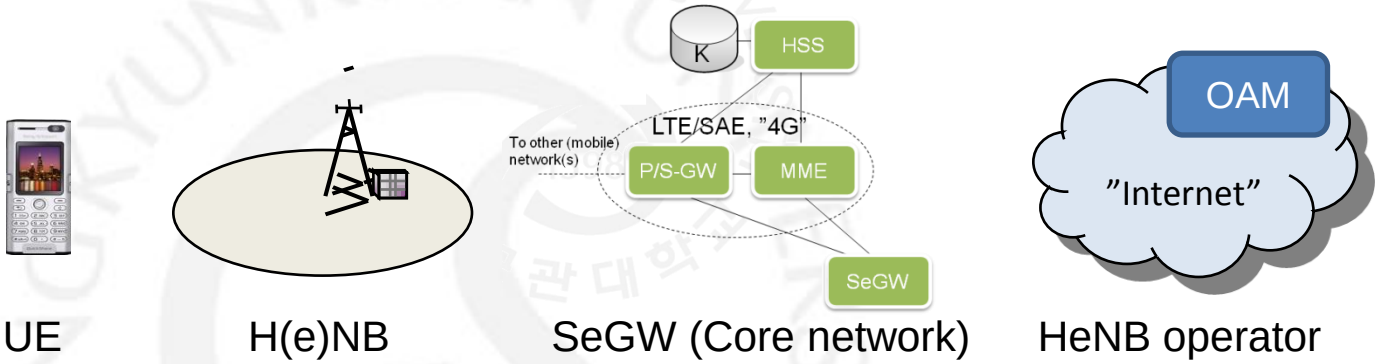
http://www.rmiclients.com/images/funnel.jpg

Threats

- Physical attacks on H(e)NB
  - Compromise HeNB authentication credentials
- Configuration attacks on H(e)NB
  - Compromise link between HNB and operator (i.e. Fraud software update)
- Protocol attacks on H(e)NB
  - Man-in-the-middle attacks
  - Threat of H(e)NB network access
- Privacy attacks on user data and identity
  - Masquerade as normal users / a valid H(e)NB

[Ref] 3rd Generation Partnership Project; Security of H(e)NB (Rel. 8), 3GPP TR 33.820 v1.3.0, Jan. 2009.

TRUST RELATION



User access control

HNB access control

Deployment agreement

Manufacturing

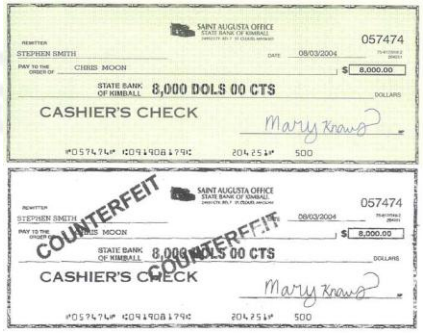
User and HNB??

Closed Subscriber Group (CSG)

Collapse of trust relation

- Rogue HNB
  - Purchase, install, and configure HeNB in open access mode
    - Sprint Airave $99 , AT&T 3G Microcell $146 (UMTS)
  - Masquerade as a normal HNB / man-in-the-middle attack
- Compromise of CSG list
  - Masquerade as a normal user
- Very harmful: Privacy, confidentiality, monetary issues

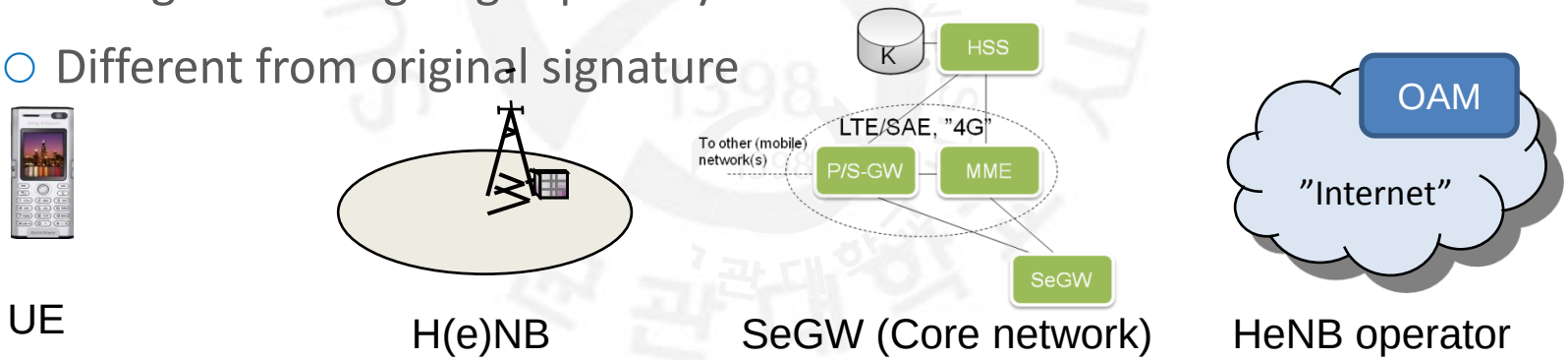
Rogue HeNB

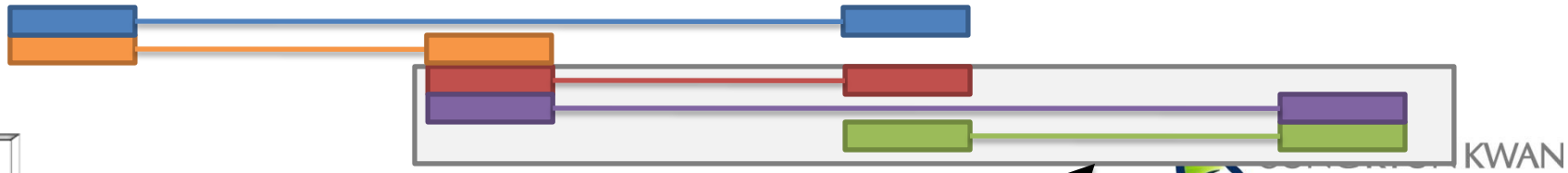


Forgery

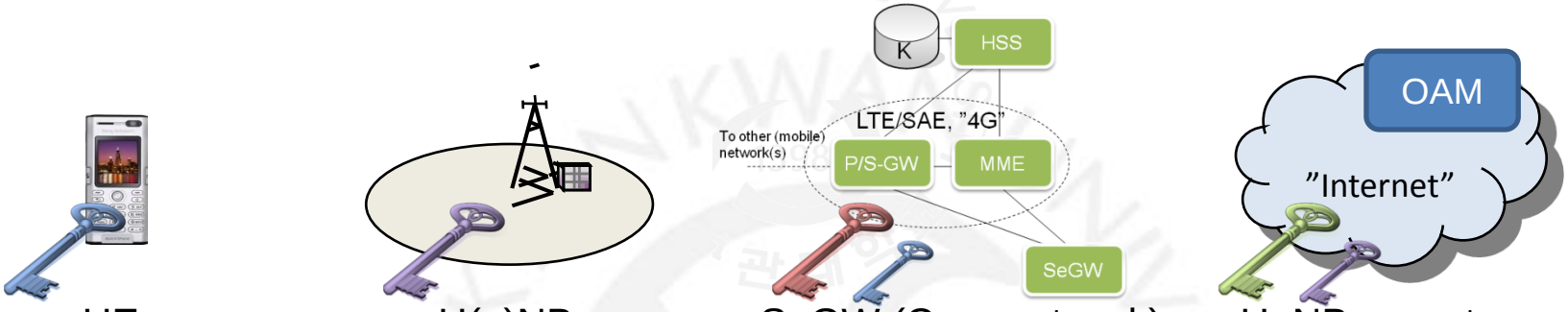
PROPOSED IDEA

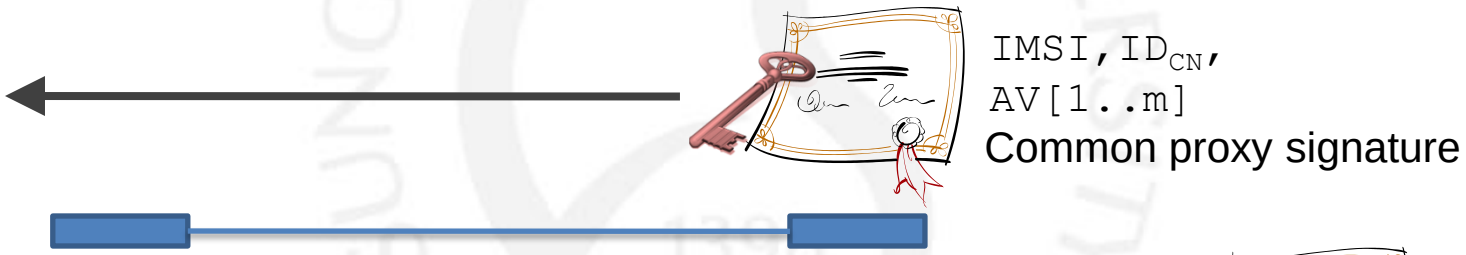
- Goal
  - To make the trust relation between UE and HNB stronger
  - To prevent the possible attack occurring
- Proxy signature
  - Delegation of signing capability
  - Different from original signature





REGISTRATION ❶

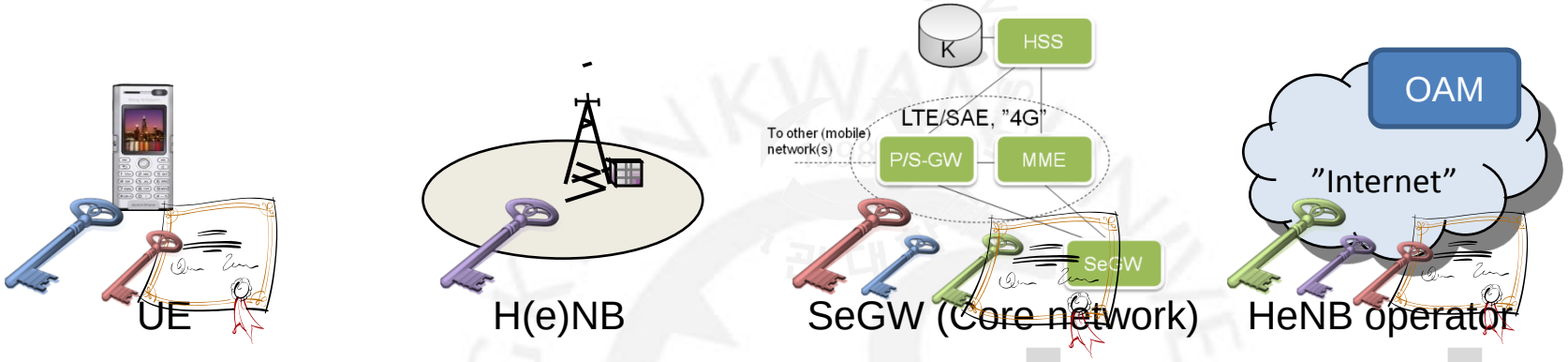




$$e = h(m_w \,||\, RAND)$$

$$\sigma_{\text{A-B}} = e \cdot s_{\text{A}} + rand \bmod q$$

REGISTRATION ②



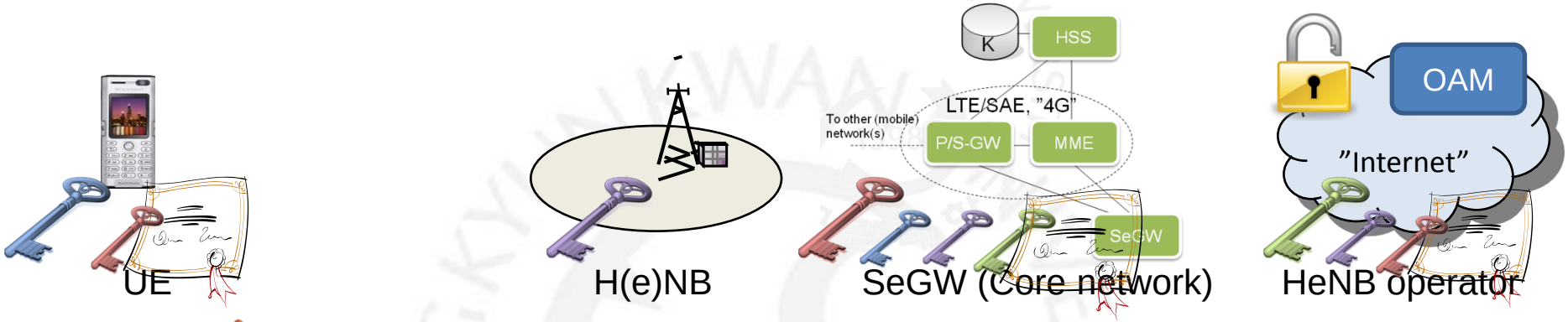
ID_{CN}, $ID_{CSGcell}$
Pub_{CN} , Pub_{HeNB}

$ID_{CSGcell}$, ID_{OAM}
Pub_{OAM}, Pub_{HeNB}

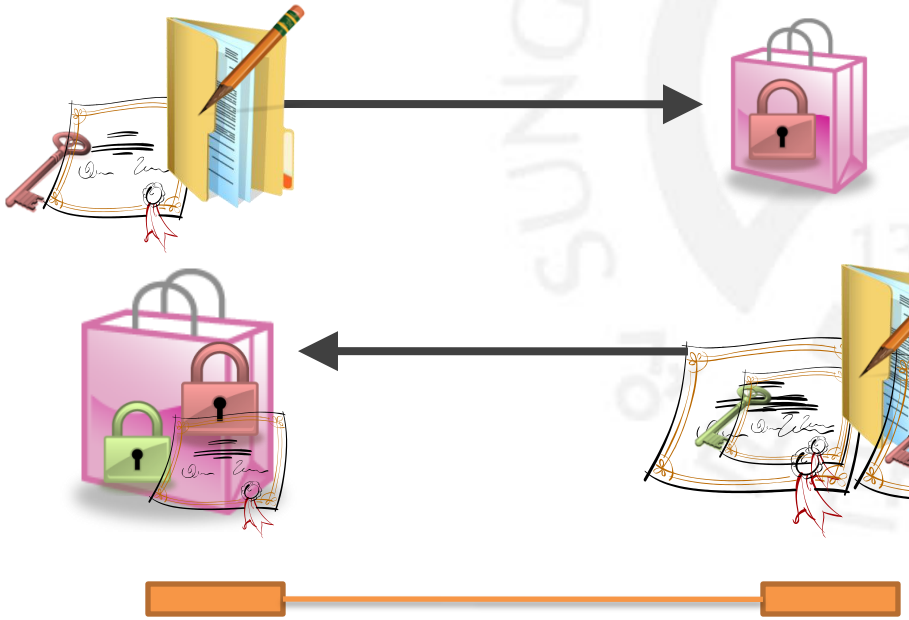
Re-delegation using proxy-signature

$$\sigma'_{B-C} = v_C \cdot k_1 + (\sigma_{\text{A-B}} + k_2) \cdot h(m_{\text{B-C}}) \bmod q$$

ACCESS CONTROL



UE H(e)NB SeGW (Core network) HeNB operator



General proxy-signed challenge
Verification: Pub_{CN}'

Generate challenge
proxy-signed proxy- + multi signature
Verification: the proxy-signed public key

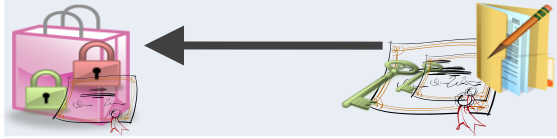
Fresh key agreement

Security analysis

- Tightly coupled trust relationship
  - More secure!
- Mutual authentication and key agreement
- Withstanding protocol attacks
  - MitM, masquerading, etc.
- Revocation of HNB
  - Temporary warrant
  - Separation of proxy-signature and re-delegated proxy-signature
- Basic properties of proxy signature
  - Unforgeability, Undeniability, Distinguishability

Performance evaluation

- No extra communication cost
  - Piggybacked on ordinary authentication phase
  - Offline, deployment, UMTS-AKA, etc.
- Computation cost
  - PolarSSL: Open source cryptographic library

Message	UE	HeNB
	2M+1H+1A	3E+3M+1H
	3E+3M+2H+1A	1M+1H+1A
Total	**+ 8.04msec**	

polarssl

E:exponentiation (0.98ms)
M:multiplication (0.00758ms)
H:hash (0.0202ms)
A:arithmetic (0.00743ms)

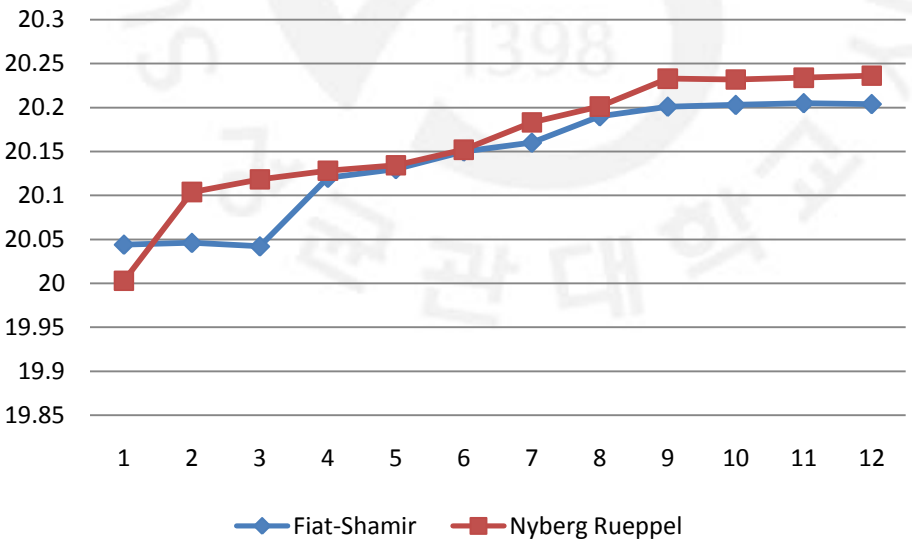
HIT

SUNG KYUN KWAN UNIVERSITY

Computational analysis

- Simulation settings
  - 1-12 user equipment, Average user equipment distance: up to 50m
  - Size of CSG list : 128 octets * # of users, Link error probability: 1%
- Total computation delay

$$T_{\text{user access control}} + T_{\text{HNB access control}} + T_{\text{CSG verification}} + T_{\text{proposed}}$$



Conclusion

- Initiative works on security of femtocell
- Proposing simple and promising solution
  - Prevention of the security threats (i.e. rouge HeNB)
- Future works
  - Key escrow problem
  - Formal security proof against various attacker model
  - Emulation of femtocell with deployment

Building Femtocell More Secure with Improved Proxy Signature

Any questions?

Chan-Kyu Han, hedwig@ece.skku.ac.kr

http://hit.skku.edu/~hedwig/

SUNG KYUN KWAN UNIVERSITY

School of Information and Communication Engineering

Computer Engineering

HIT

SUNG KYUN KWAN UNIVERSITY