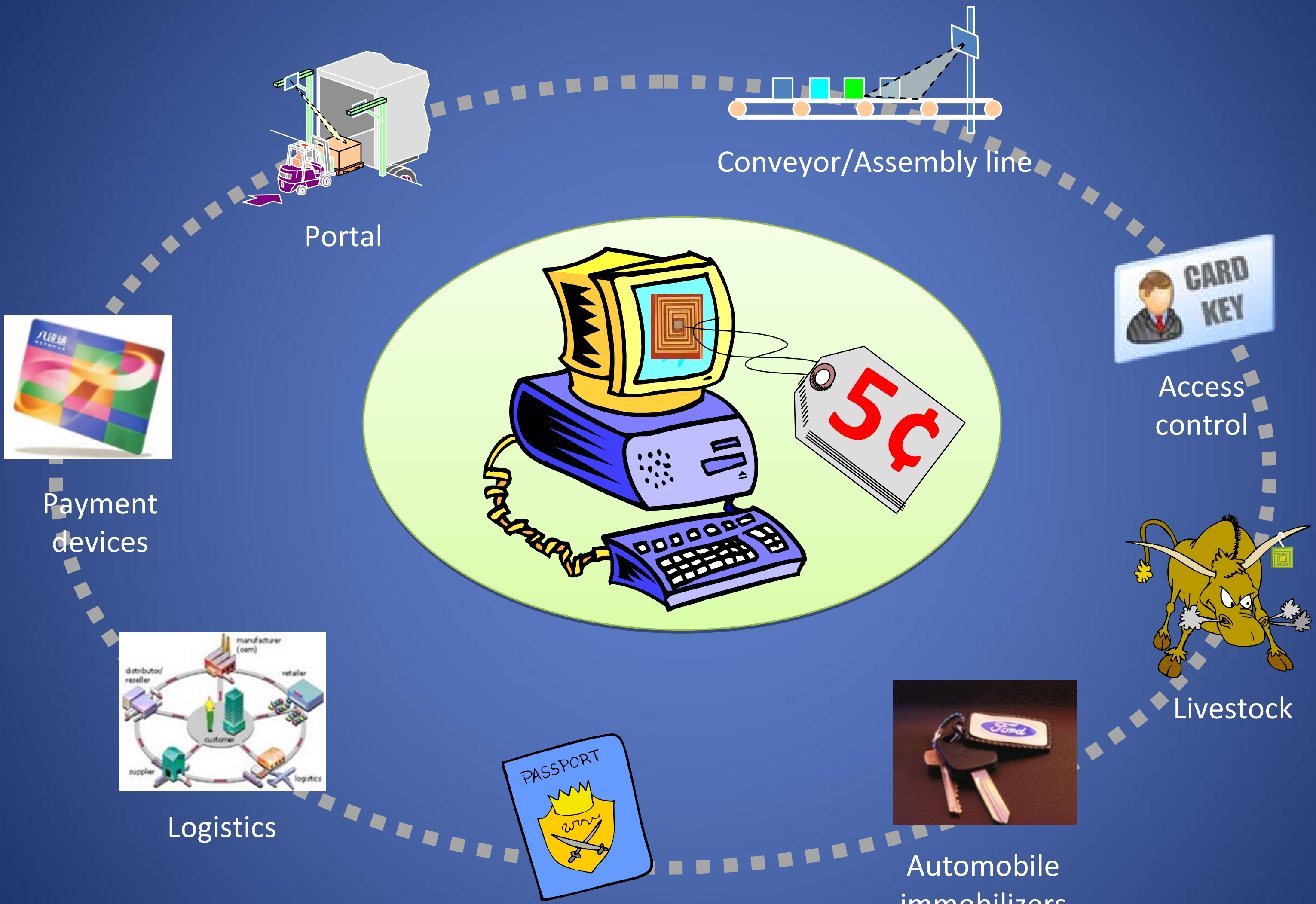
Trustworthy RFID Technologies for E-Logistics and Internet of Things
可信無線射頻標籤技術在電子物流及物聯網中之應用

韩劲松
Jinsong Han
2011.9.23

RFID Overview



Portal

Conveyor/Assembly line

Access control

Livestock

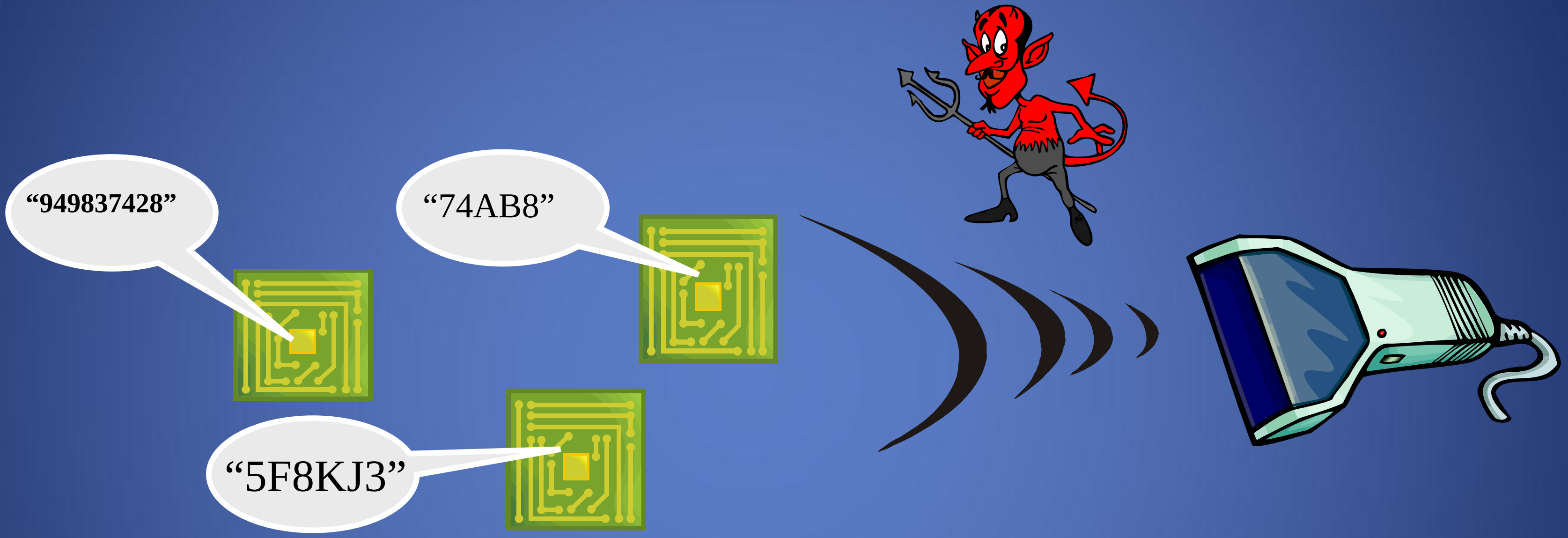
Automobile immobilizers

Passport

Logistics

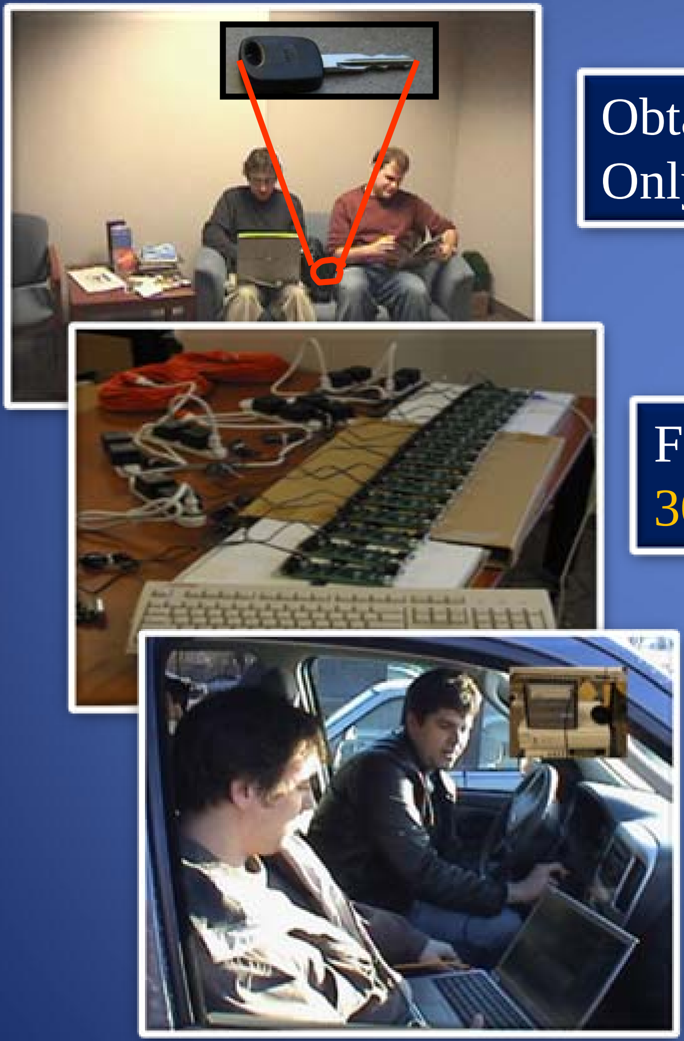
Payment devices

Privacy and Security Concerns



- Passive overhearing, cloning, compromising, etc.
- Setting a password is still not secure!

Cracking EPC Tag Password



Obtain responses from tag.
Only 1/4 second!

Find the access password
30 minutes with 16 parallel crackers!

Simulate radio signals or produce a fake tag with cracked password!

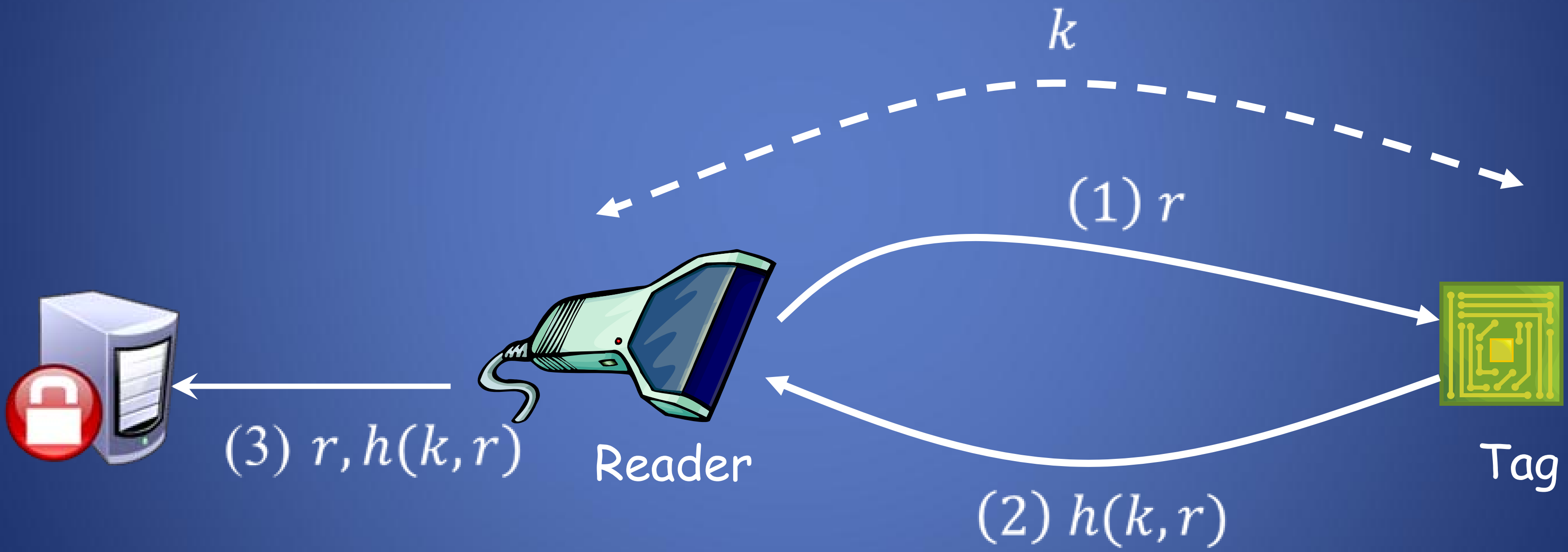
LSCM Project Overview ——GHP/044/07LP

- Phase I: Trustworthy RFID Technologies: Methodology and Practice, GHP/044/07LP, 2008-2010, done
- Ssponsored by ITF Funding
- Supervised by LSCM
- Platform research programs

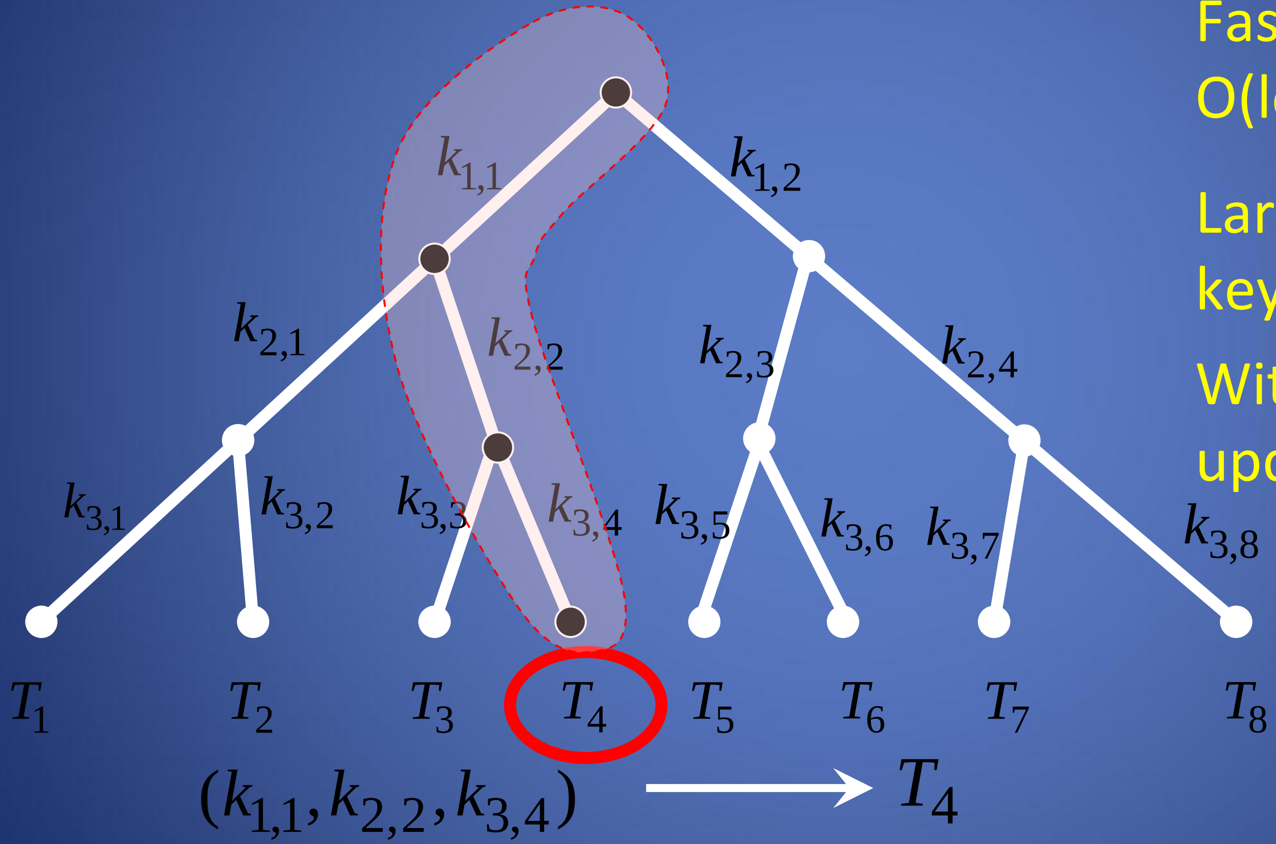
項目發展計劃

- 開發基於RFID安全技術 (Phase I)
- 加解密 (En/Decryption)
- 認證 (Authentication)
- 隱私保護 (Privacy Protection)
- 基於RFID的安全可信架構技術 (Phase II)
- 可信中心 (Trust Center)
- 信任及信用管理 (Trust management and auditing)
- 所有权转移 (Secure Ownership Transfer)
- 可信合作 (Trustworthy Collaboration)

Digital Signature based Solution



秘钥搜索



Fast and scalable, O(log*n*)

Large overhead in key-updating

Without key-updating,

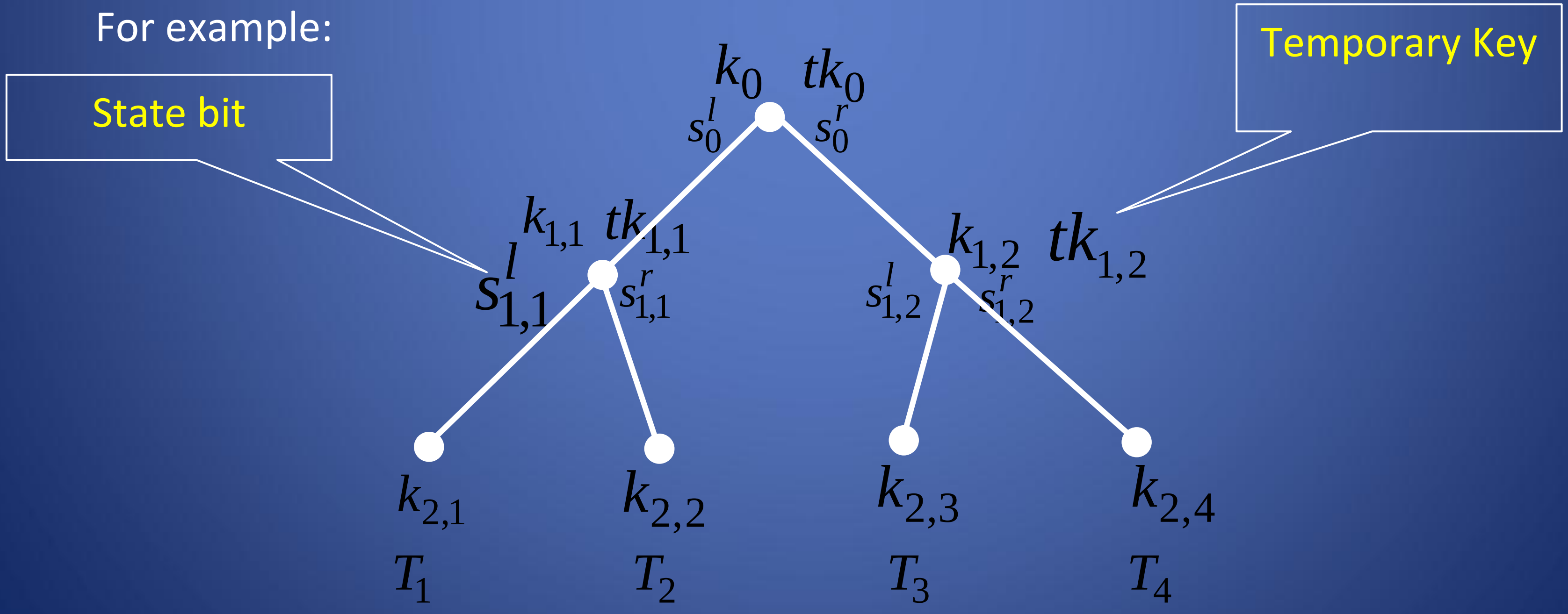
No forward security

Vulnerable to compromising attack

支持秘钥更新的认证协议： SPA

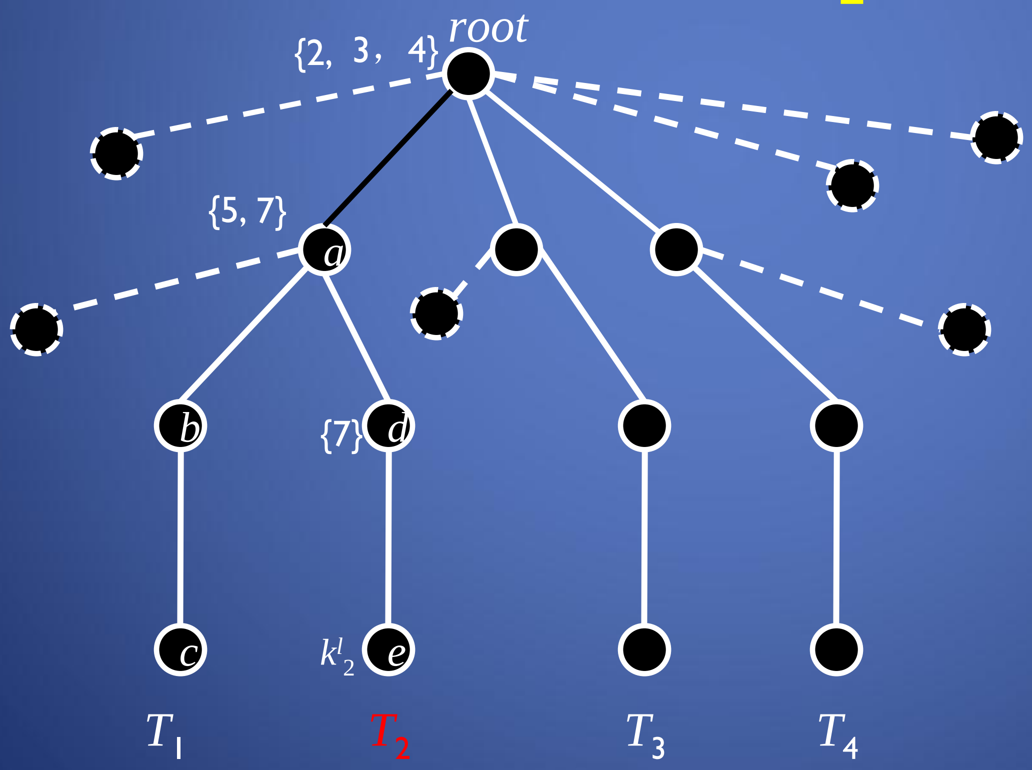
- Temporary keys are used to store old keys.
- State bits are used to record the key-updating status of nodes in the sub-trees.

For example:



ACTION: Anti-Compromising Attacks

- Sparse tree based
- For example, to identify T_2

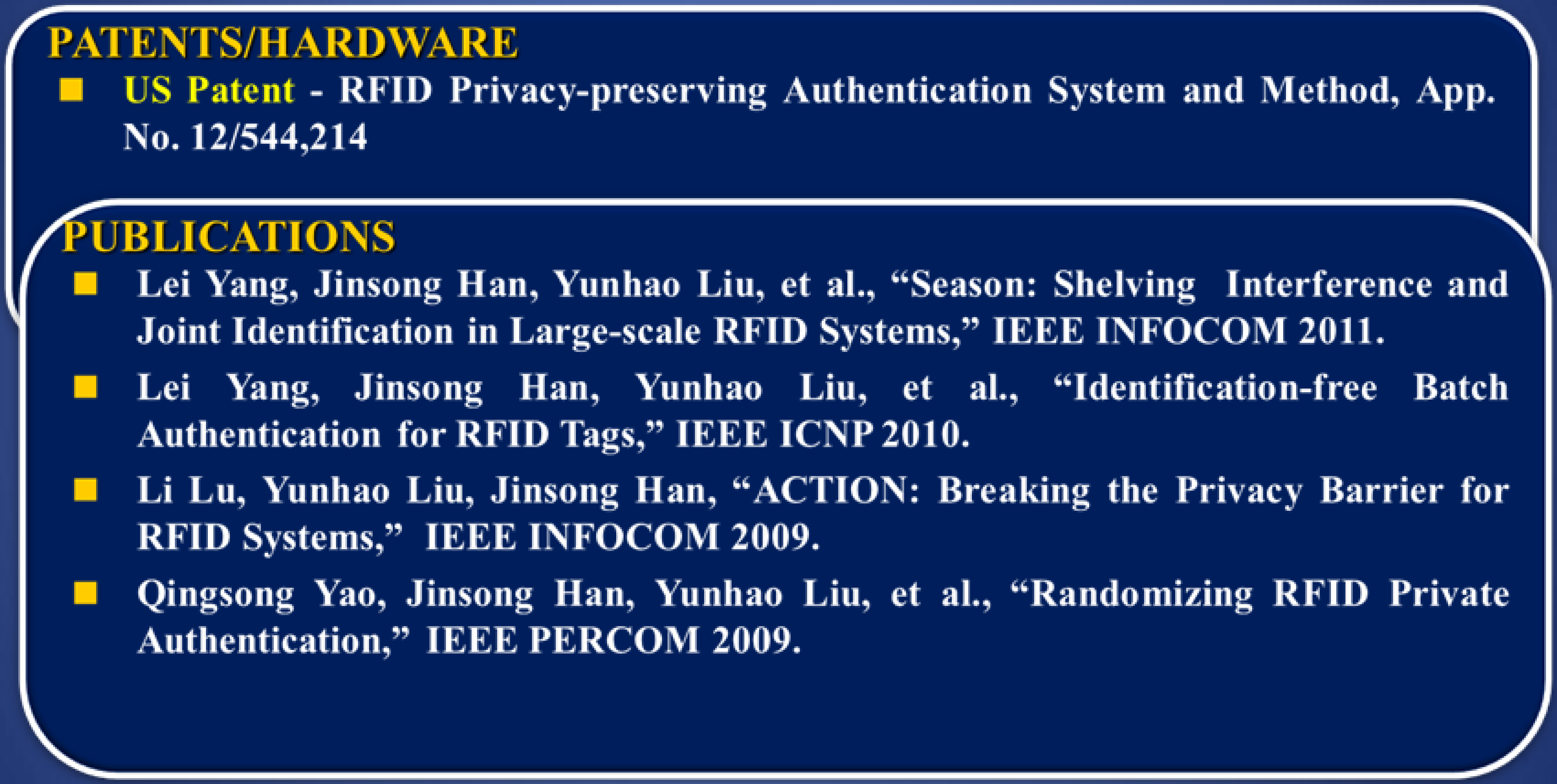


Reader sends: Request, r_1

T_2 replies: r_2, $h(r_1, r_2, 2)$, $h(r_1,r_2,7)$, $h(r_1,r_2,7)$, $h(r_1, r_2, k^l_2)$

$h(r_1, r_2, 2)$
$h(r_1, r_2, 7)$
$h(r_1, r_2, 7)$
$h(r_1, r_2, k^l_2)$

Results



PATENTS/HARDWARE

- **US Patent** - RFID Privacy-preserving Authentication System and Method, App. No. 12/544,214

PUBLICATIONS

- Lei Yang, Jinsong Han, Yunhao Liu, et al., “Season: Shelving Interference and Joint Identification in Large-scale RFID Systems,” IEEE INFOCOM 2011.
- Lei Yang, Jinsong Han, Yunhao Liu, et al., “Identification-free Batch Authentication for RFID Tags,” IEEE ICNP 2010.
- Li Lu, Yunhao Liu, Jinsong Han, “ACTION: Breaking the Privacy Barrier for RFID Systems,” IEEE INFOCOM 2009.
- Qingsong Yao, Jinsong Han, Yunhao Liu, et al., “Randomizing RFID Private Authentication,” IEEE PERCOM 2009.

Preliminary Implementation

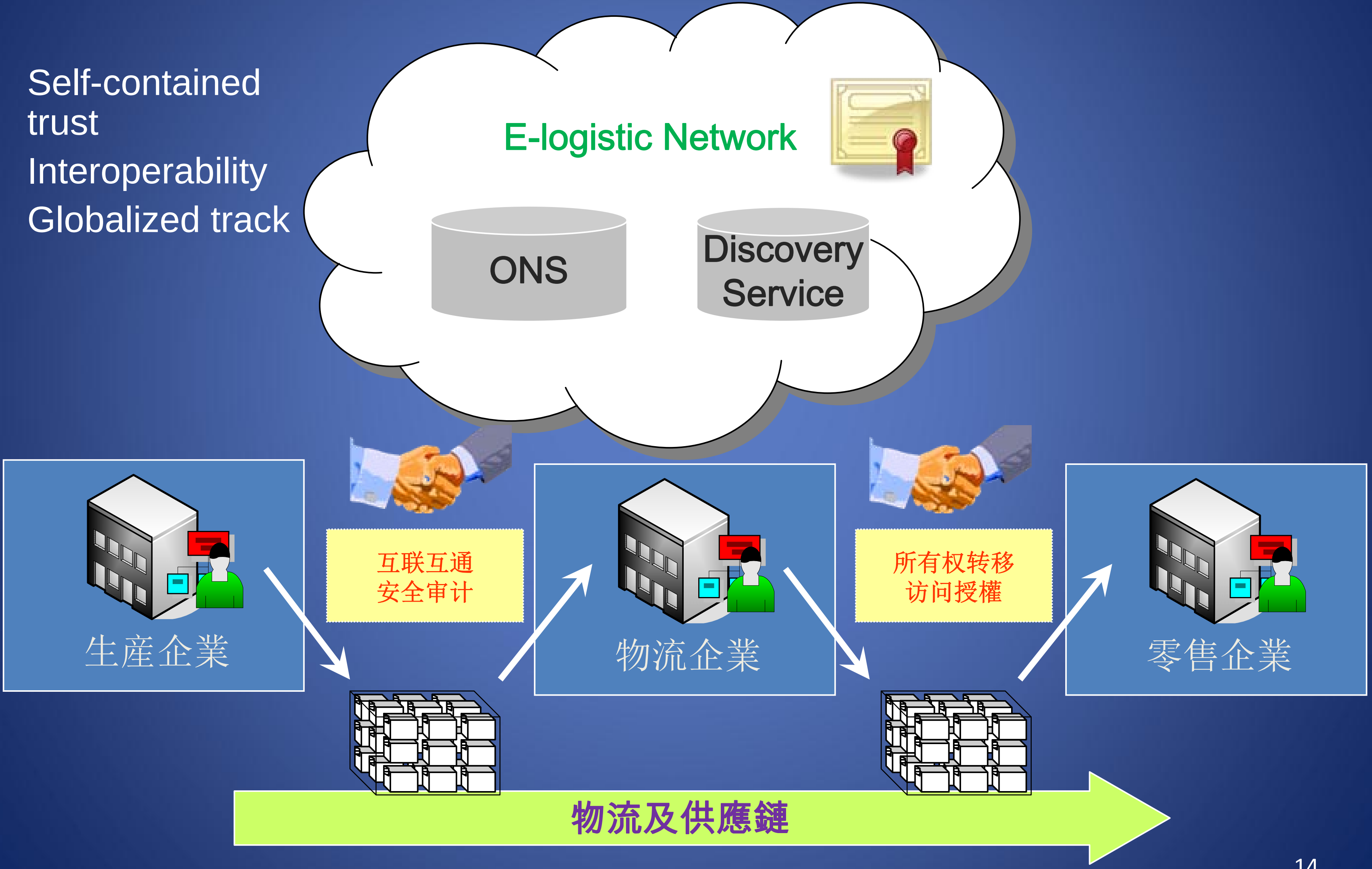
- Preliminary implementation in Xi'an Postal Processing Center
  - One of the 7 key-processing centers in China
  - 20 million packages of mails, 640 million letters, 32 million flat mails, 10.8 million parcel-like mails per year.
- gi

LSCM Project Overview ——ITP/037/09LP

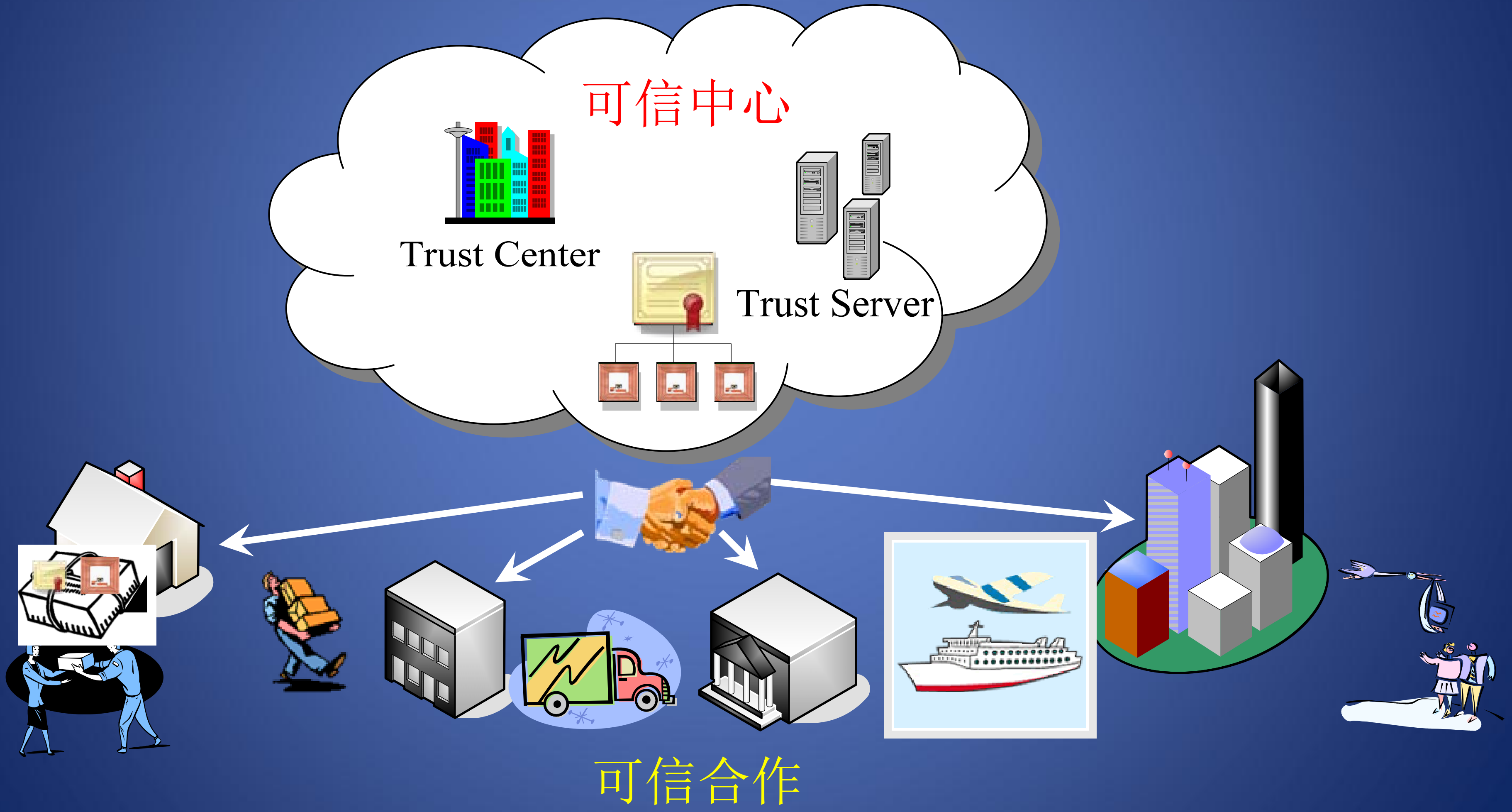
- Phase II: Trust Solution for RFID Enabled Interoperable E-logistics, ITP/037/09LP, 2010-2012, ongoing
- Sponsored by ITF Funding
- Supervised by LSCM
- Platform research programs

安全电子物流

- Self-contained trust
- Interoperability
- Globalized track



面向RFID的可信安全架构技术



防伪需求

海關打擊冒牌藥物		
事項	2009年	2010 年
案件	46宗	22宗
檢獲藥物數量	71417件	55080件
檢獲藥物總值	HK$ 332 萬元	HK$ 495萬元
被捕人數	50人	37人
冒牌西藥投訴	62宗	28宗

Hong Kong Customs seized 55,000 fake drugs, worth around 5M HK$ in 2010.

China loses about 600 billion per year due to fake goods.

According to the WHO, 7 - 10% of the world's pharmaceuticals are counterfeit in developed countries, 25%~50% in developing countries.

Online counterfeit sales will cost businesses $135 billion in 2011

- Internet retailer

5% of world trade!

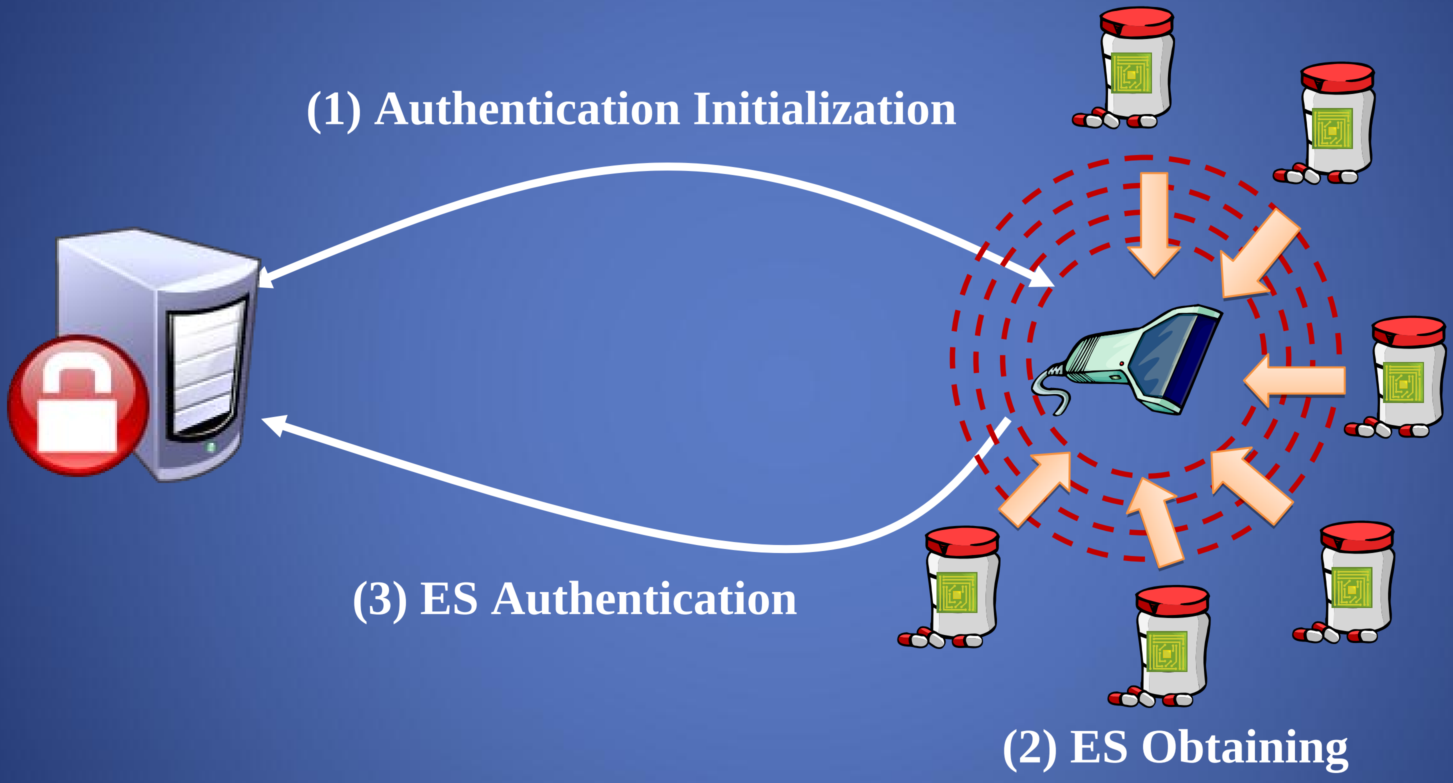
RFID 防伪技术的瓶颈 – 逐一认证

ULTRA THIN PORTABLE SPACE SUITS

- Anti-Collision
- Per-tag Authentication

- Low efficient Identification
- High volume of authentication data
- Significant server workload

Single Echo based Batch Authentication (SEBA) - Overview



(1) Authentication Initialization

(3) ES Authentication

(2) ES Obtaining

The reader abstracts the response results as Echo Sketch.

Dissemination

- **Hong Kong ICT Awards 2011**: Best Innovation & Research Award competition, with the entry, “Identification-Free Batch Authentication for RFID Tags”, Feb 19, 2011.
  - Granted the Silver Award in the Postgraduates & Open stream.
  - Four rounds of competition.

TION CEREMONY 頒獎典禮 15.4.2011
formation Officer
inistrative Region
rade Development Council
香港特別行政區政府 政府資訊科技總監辦公室
LuxonDATA

HONG KONG ICT AWARDS
2011 香港資訊及通訊科技獎
AWARDS PRESENTATION CEREMONY 頒獎典禮 15.4.2011

HONG KONG ICT AWARDS 2011
HONG KONG ICT AWARDS 2011 :
BEST INNOVATION & RESEARCH
(POSTGRADUATES & OPEN)
Silver Award
Han Jinsong, Liu Yunhao, Yang Lei
iProA

Conclusion

- Trustworthy and privacy-preserving RFID computing
- Internet of things (IOT)
- Any time, Anywhere, Any service

Thanks!