KRACK & ROCA

吳忠憲 [1,3] 陳君明 [1,2,3]

J.-S. Wu Jimmy Chen

1. NTU, National Taiwan University
2. IKV, InfoKeyVault Technology
3. CHROOT & HITCON

Agenda

- **KRACK** – **K**ey **R**einstallation **A**tta**ck**s
  - Serious weaknesses in WPA2, a protocol that secures all modern protected Wi-Fi networks
- **ROCA** – **R**eturn **o**f **C**oppersmith's **A**ttack
  - A vulnerability in the implementation of RSA key pair generation in a cryptographic library used in a wide range of cryptographic chips

國立臺灣大學 National Taiwan University

KRACK

14 Years of WWPA/WPA2

- ~~1997: WEP (completely broken)~~
- 2003: WPA
- 2004: WPA2
- Many attacks against Wi-Fi, but
- Handshake & encryption remain "secure"
  - Until 2017
  - KRACK discovered by Mathy Vanhoef

國立臺灣大學 National Taiwan University

GOOGLE \ TECH \ ANDROID

82

41 percent of Android phones are vulnerable to 'devastating' Wi-Fi attack

Every Wi-Fi device affected by some variant of attack

by Tom Warren | @tomwarren | Oct 16, 2017, 5:54am EDT

SHARE TWEET LINKEDIN

10 CVE IDs for KRACKs

- Targeting different aspects of WPA/WPA2
  - CVE-2017-130{77,78,79,80,81}
  - CVE-2017-130{82,84,86,87,88}

國立臺灣大學 National Taiwan University

10 CVE IDs for KRACKs

- Targeting different aspects of WPA/WPA2
  - CVE-2017-130{**77**,78,79,80,81}
  - CVE-2017-130{82,84,86,87,88}

- Let's see how to *KRACK* the 4-way handshake

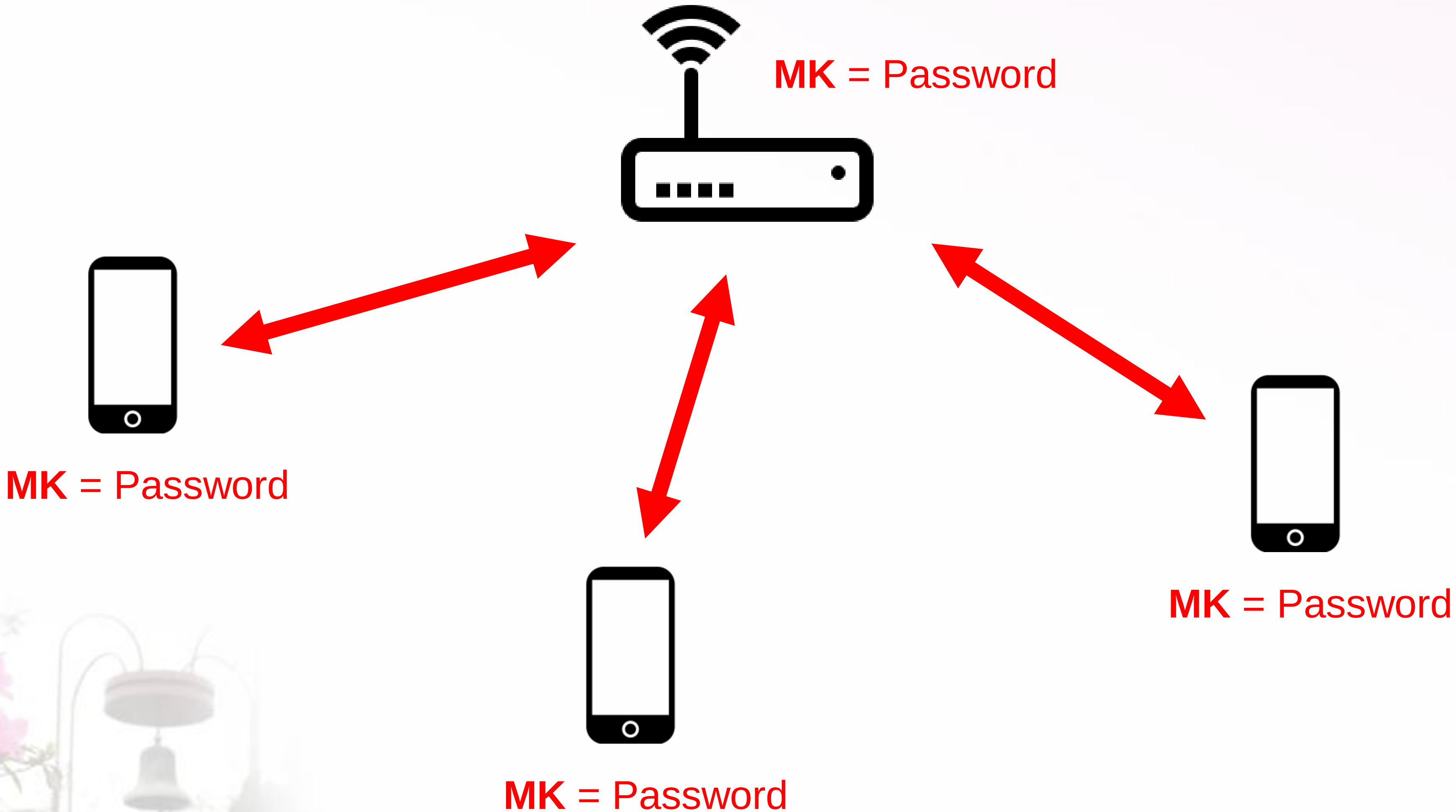
國立臺灣大學 National Taiwan University

Before the 4-way Handshake

- A client and an AP need to setup a shared secret master key **MK**

國立臺灣大學 National Taiwan University

“Personal” Network

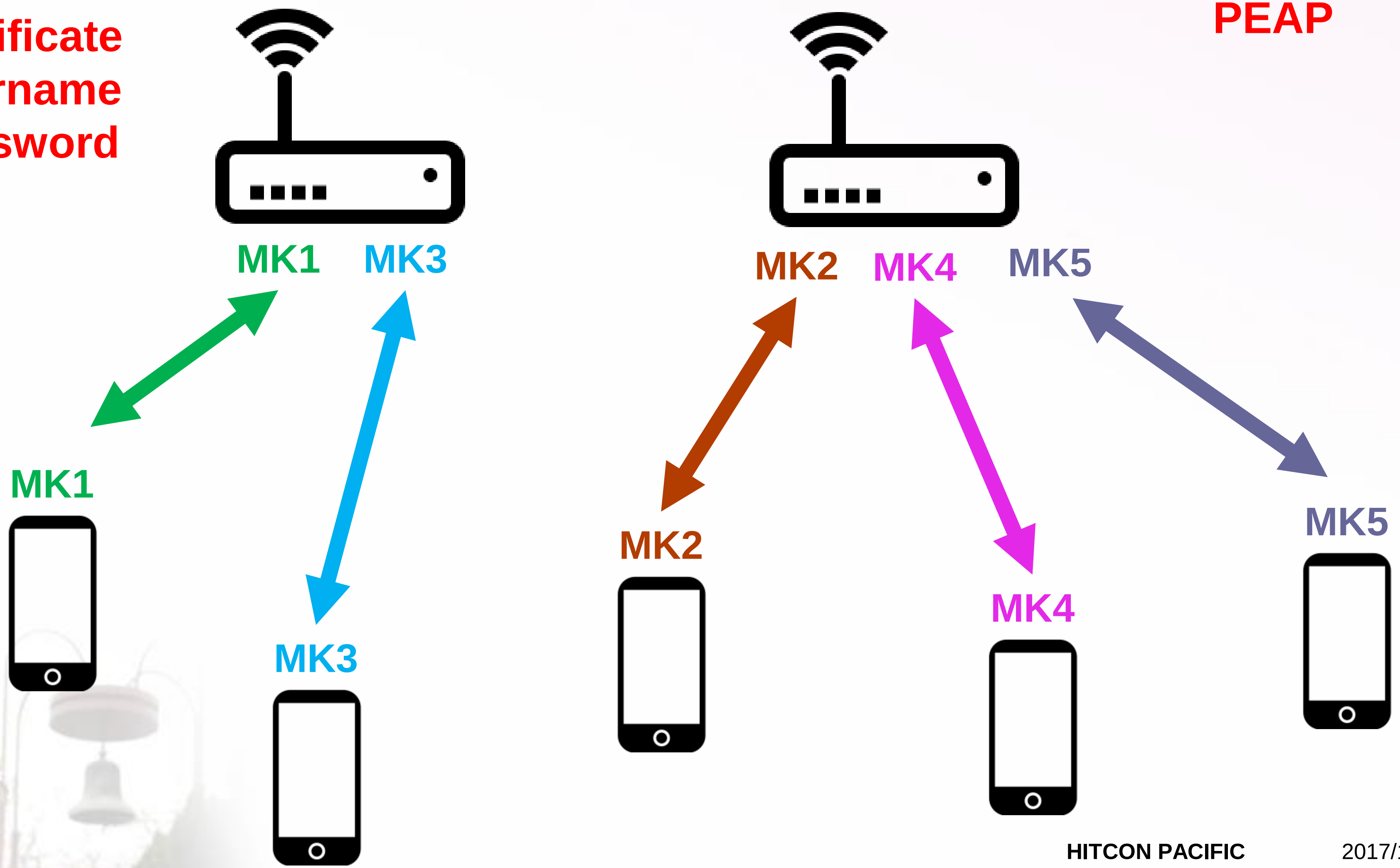


國立臺灣大學 National Taiwan University

"Enterprise" Network

802.1X
PEAP

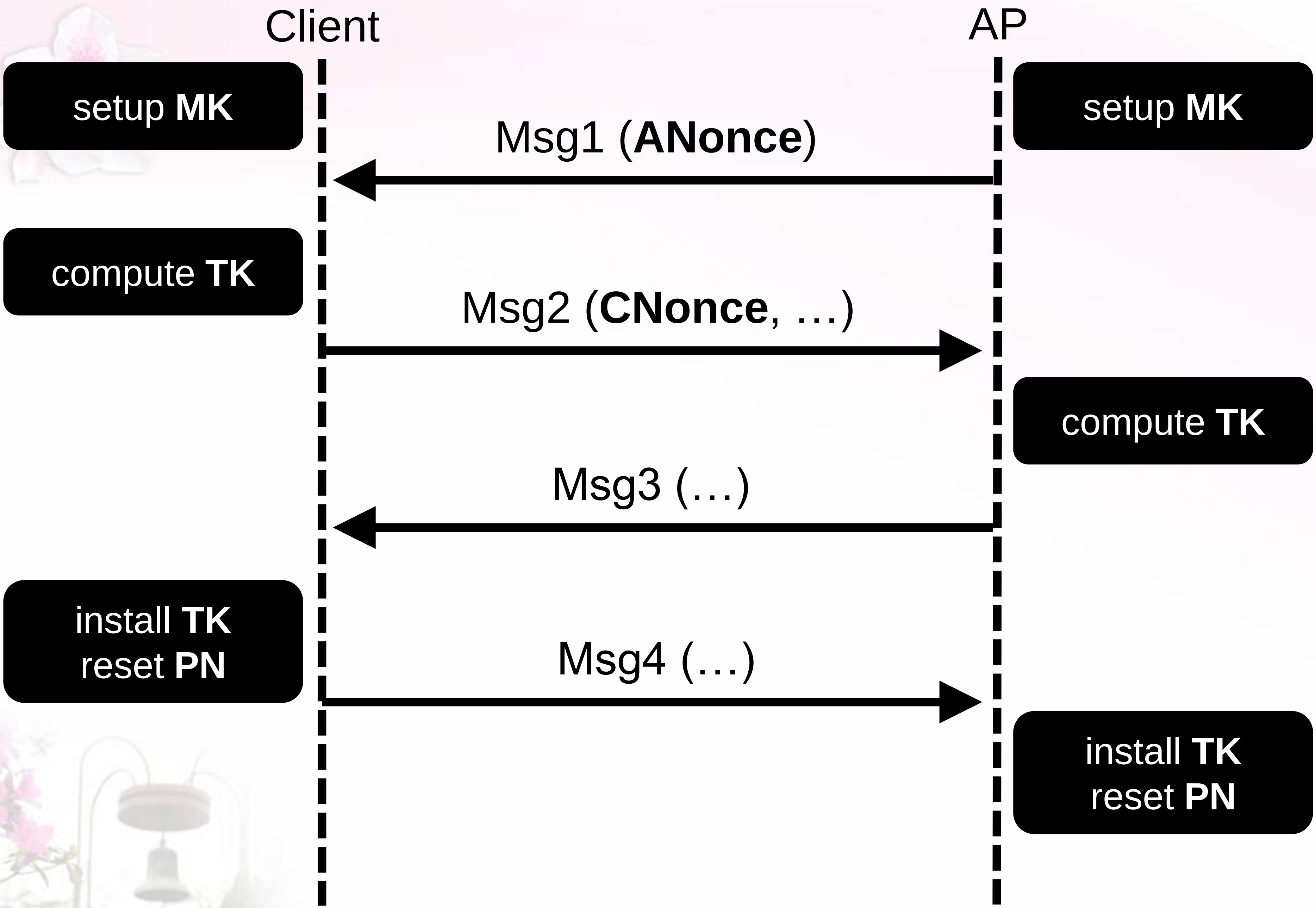
Certificate
Username
Password



The 4-way Handshake

- Based on a shared **MK** between an AP and a client…
- Mutual authentication
- Negotiate a fresh temporal key **TK**
  - for actual encryption
  - can be refreshed

國立臺灣大學 National Taiwan University



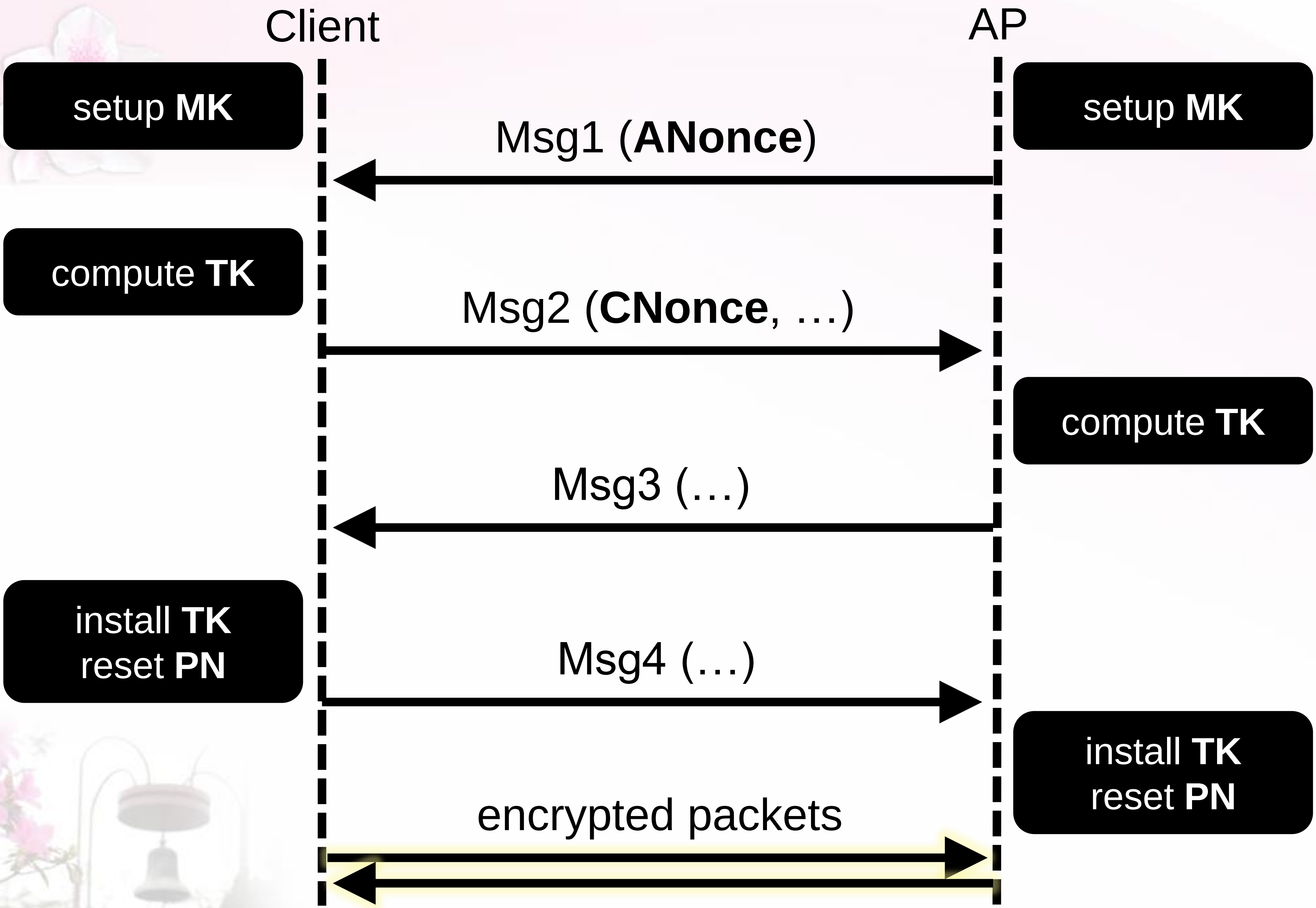
Client
AP
setup **MK**
setup **MK**
Msg1 (**ANonce**)
compute **TK**
Msg2 (**CNonce**, …)
compute **TK**
Msg3 (…)
install **TK**
reset **PN**
Msg4 (…)
install **TK**
reset **PN**

WPA2 Wi-Fi Encryption

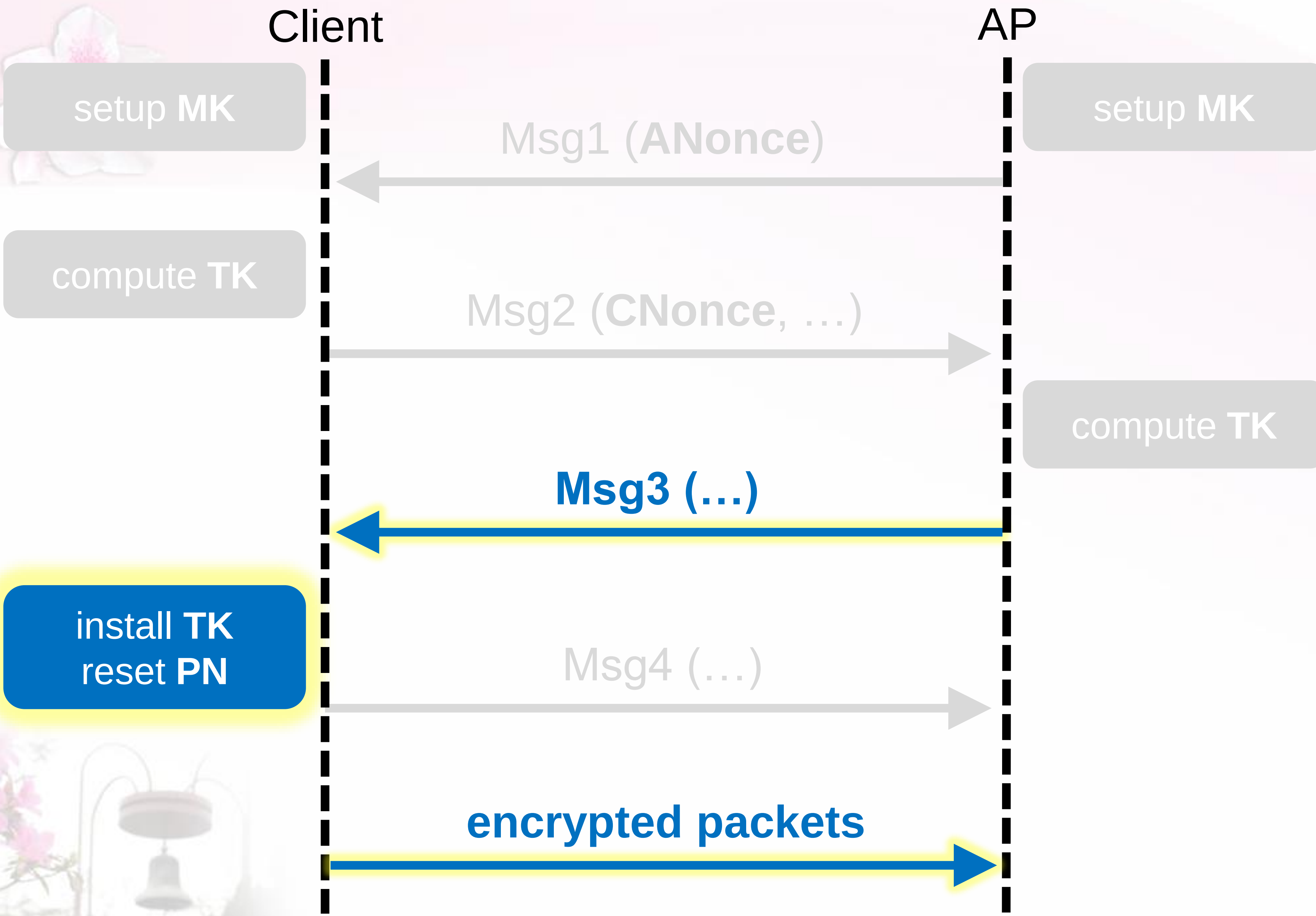
- 3 parameters are ***installed*** on both ends
  - the temporal key **TK**
  - the **RxPN** (replay counter)
  - the **TxPN** (encryption nonce)

- Using CCM or GCM with AES-128
  - **TK** is the encryption key

國立臺灣大學 National Taiwan University



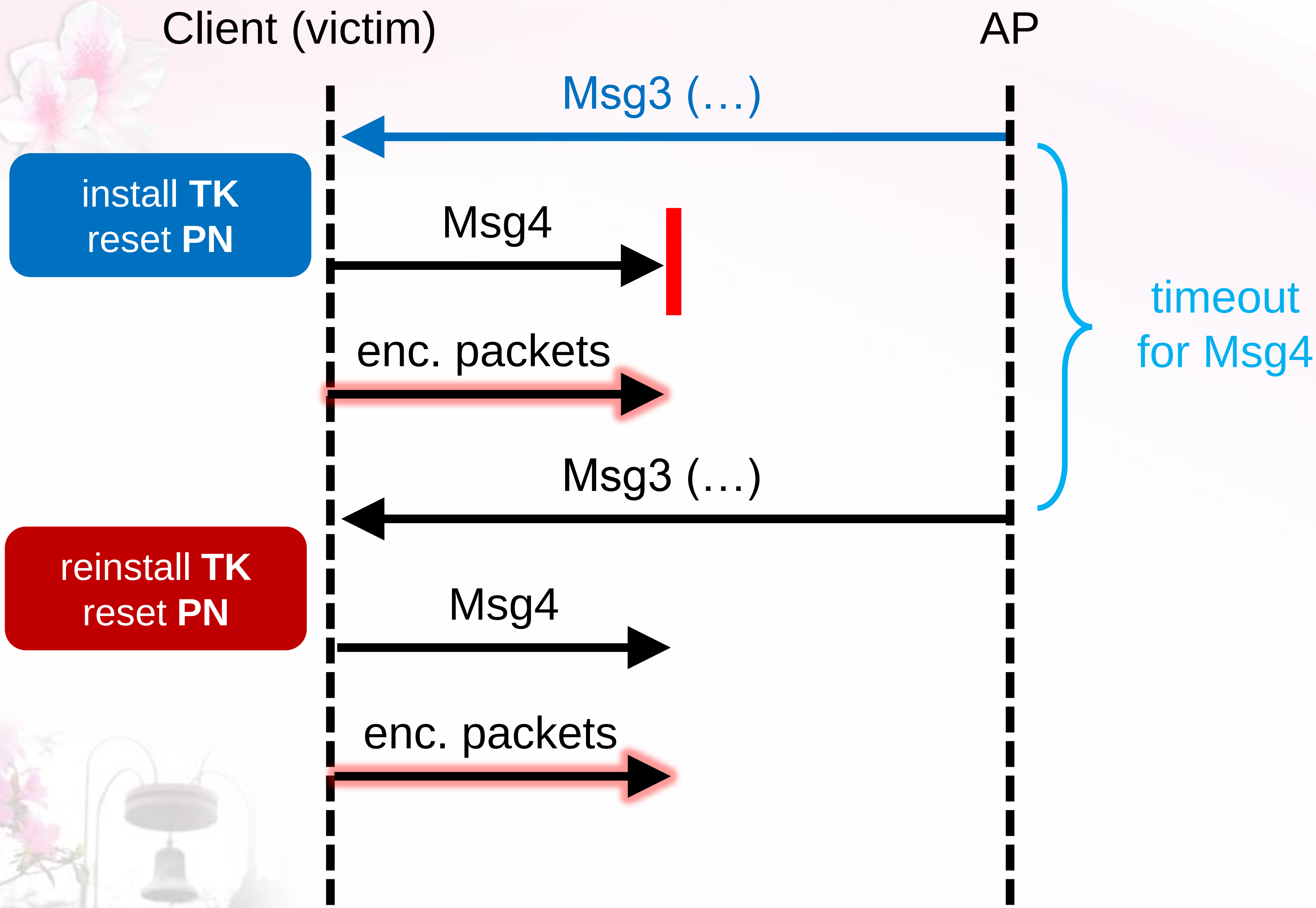
國立臺灣大學 National Taiwan University


Client
AP
setup **MK**
setup **MK**
Msg1 (**ANonce**)
compute **TK**
Msg2 (**CNonce**, …)
compute **TK**
Msg3 (…)
install **TK**
reset **PN**
Msg4 (…)
encrypted packets

Key Reinstallation

- Under the same secret key…
- If encryption nonce (TxPN) gets reset:
  - packets can be decrypted
  - packets can be spoofed (for GCM)
- If replay counter (RxPN) gets reset:
  - packets can be replayed

國立臺灣大學 National Taiwan University



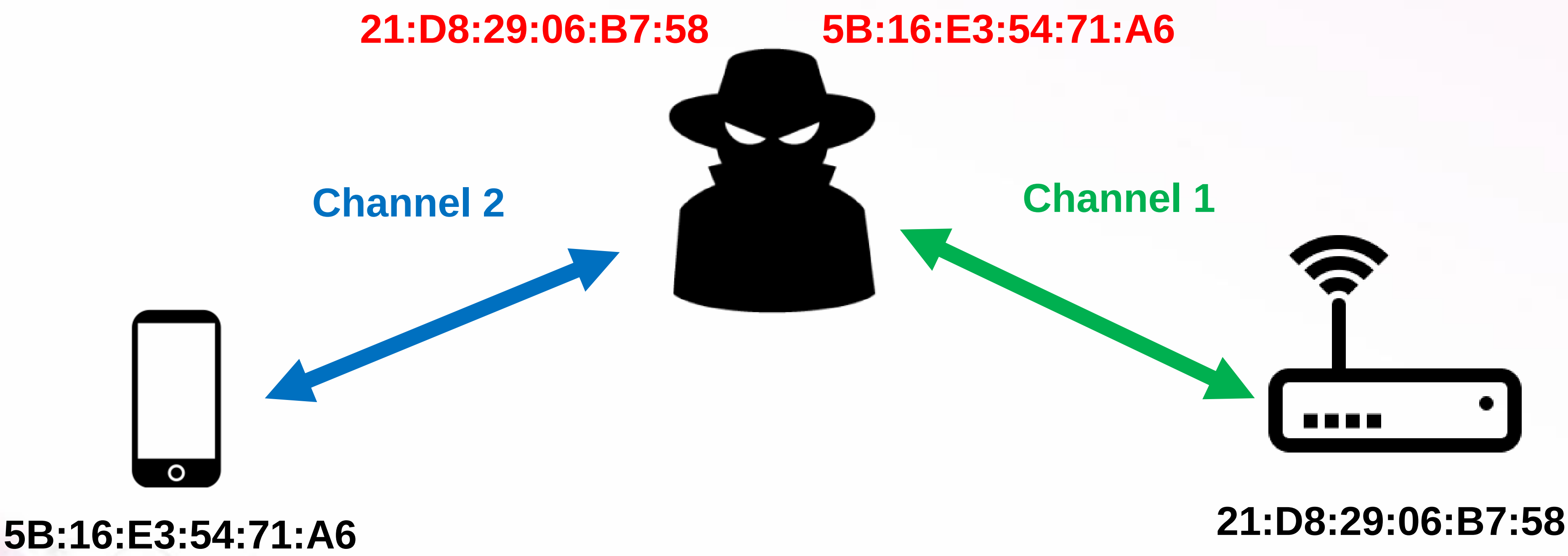
國立臺灣大學 National Taiwan University

Reinstall an All-Zero Key

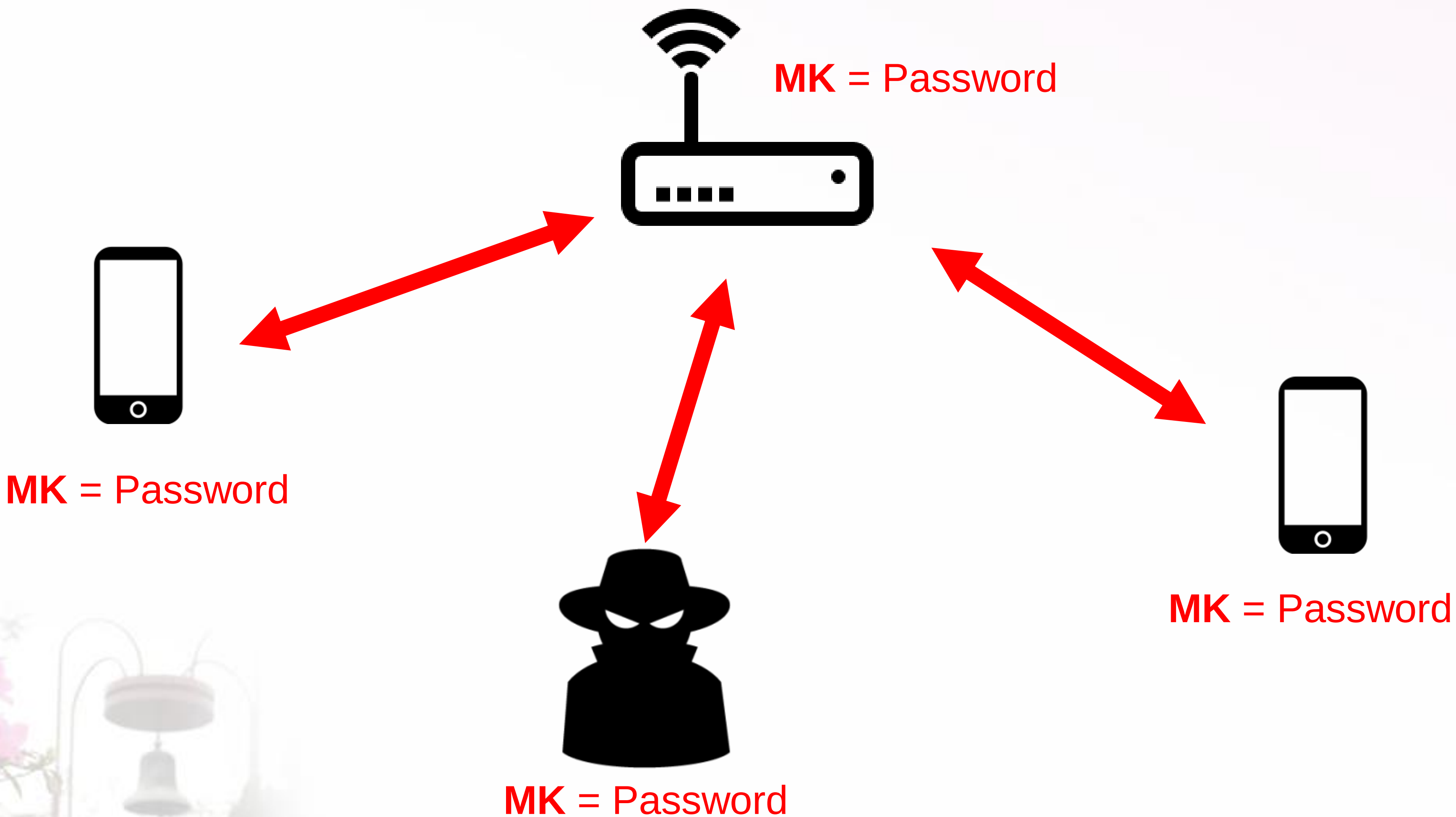
- A serious bug found in wpa_supplicant
- Android 6.0+ and Linux

國立臺灣大學 National Taiwan University

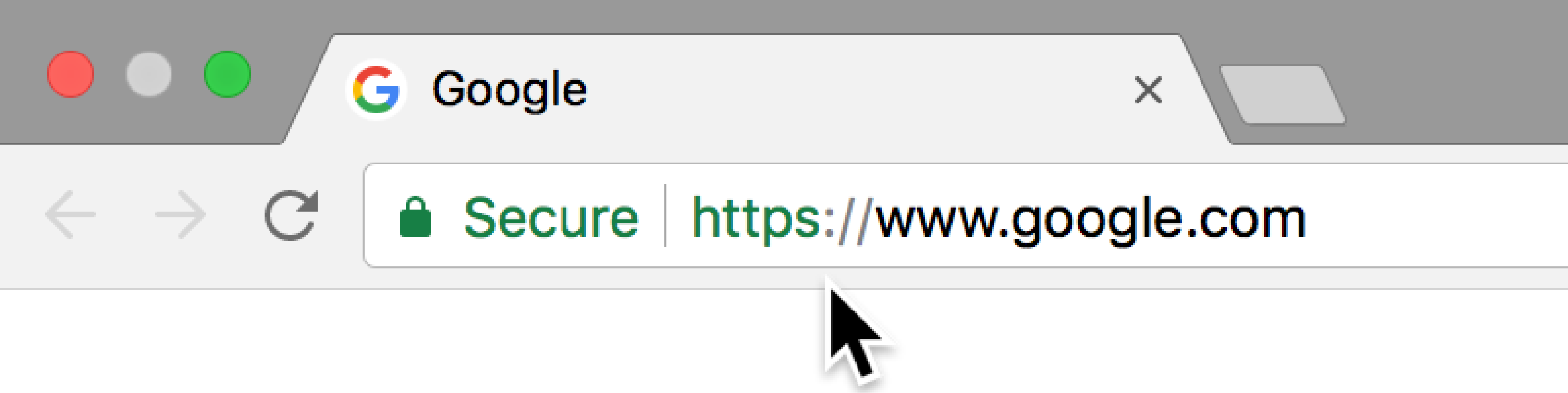
Man-in-the-Middle



Many Networks are “Unaffected” by KRACK



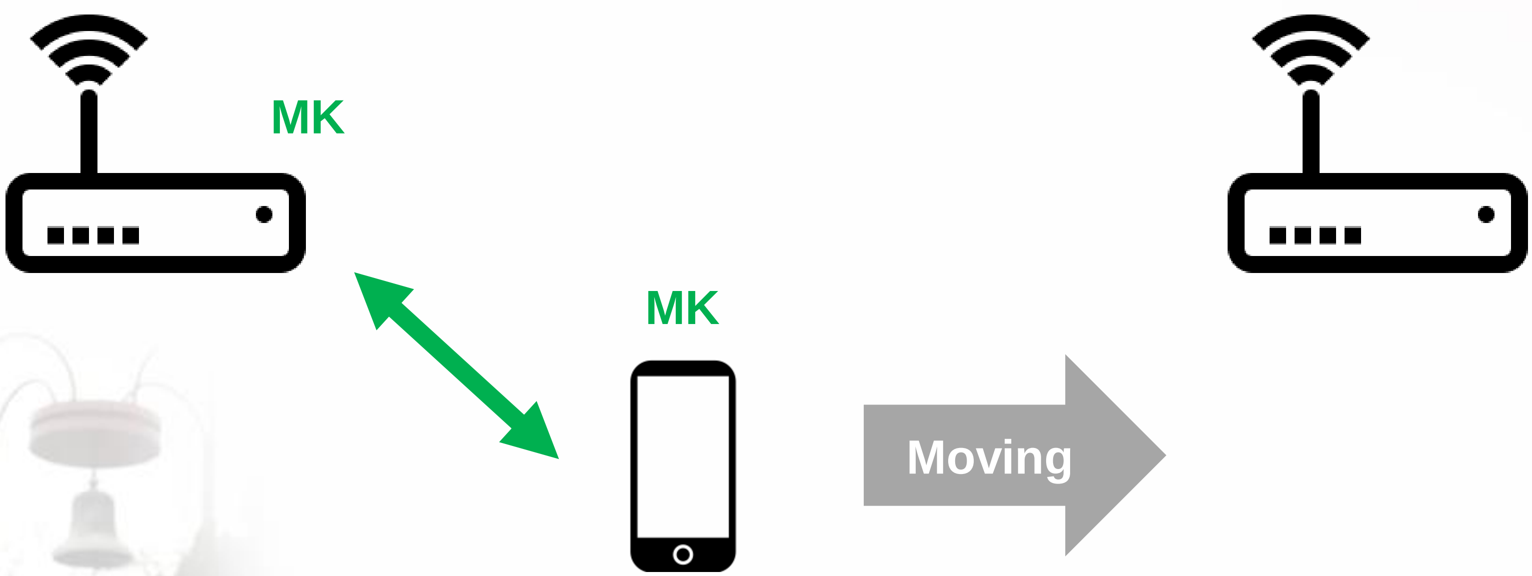
國立臺灣大學 National Taiwan University



Properly configured HTTPS, TLS, VPN… are unaffected too

KRACK the Wi-Fi Fast Roaming

- **Enterprise** networks with multiple APs
  - clients are moving
- FT (**F**ast **T**ransition) handshake

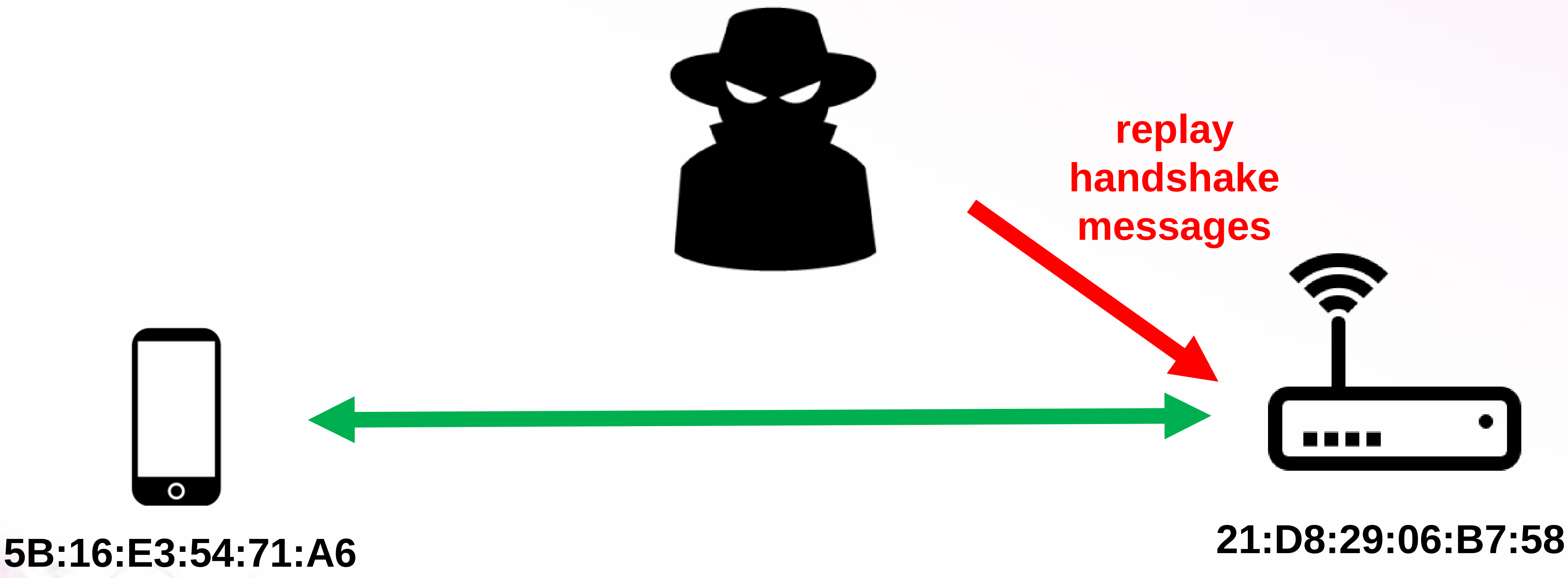


國立臺灣大學 National Taiwan University

KRACK the Wi-Fi Fast Roaming

- **Enterprise** networks with multiple APs
  - – clients are moving
- FT (**F**ast **T**ransition) handshake
  - – similar reinstallation issue on *the AP side*
  - – no replay counter at all
  - – **more exploitable!!!**

No MitM Needed to KRACK FT



The Root Cause of KRACK

- The IEEE 802.11 standards didn’t specify the precise behaviors

- Previous formal analyses didn’t model “key installation”
  - 4-way handshake proven secure
  - CCM/GCM encryption proven secure

國立臺灣大學 National Taiwan University

Fix the KRACK Vulnerabilities

- **Both** clients and APs need patches
  - Android 6.0+ and Linux devices!
  - APs in **enterprise** networks!

- Don't do the harmful key reinstallation
- Mitigate at the other end

國立臺灣大學 National Taiwan University

Lessons Learned (1/2)

- Good spec & correct code
- Abstract model vs. reality

國立臺灣大學 National Taiwan University

Lessons Learned (2/2)

- What if some part of your infrastructure is compromised?
  - control the threats

- Encrypt everything properly in transit
  - don’t assume enough (if any) security from (wireless) LAN
  - HTTPS, TLS, VPN

國立臺灣大學 National Taiwan University

ROCA

國立臺灣大學 National Taiwan University

Crypto Flaws on Chips

- EasyCard (悠遊卡) / Mifare Classic, *NXP*, 2008
- Citizen Certificate (自然人憑證), *Renesas*, 2013
  - "Coppersmith in The Wild"
- Devices around the world, *Infineon*, 2017
  - "Return of Coppersmith's Attack (ROCA)"
  - CVE-2017-15361

國立臺灣大學 National Taiwan University

EasyCard / Mifare – NXP

- The "Mifare Classic" RFID chip is used in hundreds of transport systems — London, Boston, Los Angeles, Amsterdam, Taipei, Shanghai, Rio de Janeiro — and as an access pass in thousands of companies, schools, hospitals, and government buildings all over the world
- The group that broke Mifare Classic is from Radboud University Nijmegen in the Netherlands
- The security of Mifare Classic is terrible — kindergarten cryptography

Source: Schneier on Security
https://www.schneier.com/blog/archives/2008/08/hacking_mifare.html

國立臺灣大學 National Taiwan University

EasyCard / Mifare – NXP

- NXP called disclosure of the attack “irresponsible”, warned that it will cause “immense damages”
- The Dutch court would have none of it: “Damage to NXP is not the result of the publication of the article but of the production and sale of a chip that appears to have shortcomings”
- NXP Semiconductors lost the court battle to prevent the researchers from publishing

Source: Schneier on Security
https://www.schneier.com/blog/archives/2008/08/hacking_mifare.html

國立臺灣大學 National Taiwan University

EasyCard / Mifare – NXP

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video 研討會

新聞

https://www.ithome.com.tw/node/63075

臺大電機教授示範無線竄改悠遊卡金額

Mifare的晶片卡安全性遭到挑戰，除悠遊卡外，也有晶片卡專家揭露晶片金融卡使用Web ATM設計瑕疵帶來的風險，連超商的Kiosk機臺都可透過PDF漏洞入侵

文/ 黃彥棻 | 2010-09-01 發表

讚 4.5 萬 按讚加入iThome粉絲團 讚 0 分享 G+

重點

- 包括晶片金融卡、悠遊卡等安全產品的安全性遭質疑
- 網路ATM傳輸過程採明碼傳輸，徒增安全風險
- 駭客利用PDF漏洞入侵超商Kiosk機臺

在日前舉辦的第六屆臺灣駭客年會（HIT 2010）中，揭露許多採用NXP公司推出的Mifare卡的產品的安全性風險。

EasyCard / Mifare – NXP

駭悠遊卡 判2年緩刑5年

2013-03-02

http://news.ltn.com.tw/news/society/paper/658204

〔記者黃立翔、張慧雯／台北報導〕號稱「不可能被破解」的台北捷運悠遊卡，前年遭敦陽科技資安顧問吳東霖破解，士林地院昨以他意在破解技術而非牟利，依變造電子票證罪判刑2年，緩刑5年，賠償悠遊卡公司100萬元，並向檢方指定的機構，提供240小時的電腦資訊教育訓練。

悠遊卡公司公關室科長陳志豪說，希望此案能起警惕之效，並重申悠遊卡系統非常可靠，竄改悠遊卡程式，馬上就會被系統察覺，勿以身試法。

判決書指，敦陽科技資安顧問吳東霖（23歲）前年5月間，找到破解悠遊卡加密的程式，自製感應線圈，將3張悠遊卡儲值金額各改為9000元（儲值上限）。

Crypto Flaws on Chips

- EasyCard (悠遊卡) / Mifare Classic, *NXP*, 2008
- Citizen Certificate (自然人憑證), *Renesas*, 2013
  - "Coppersmith in The Wild"
- Devices around the world, *Infineon*, 2017
  - "Return of Coppersmith's Attack (ROCA)"
  - CVE-2017-15361

國立臺灣大學 National Taiwan University

Citizen Certificate – Renesas

- The Renesas HD65145C1 chip is a "High-Security 16-bit Smart Card Microcontroller" used in many high-security applications, including banking
- This chip received a certificate, that certifies the chip was conformant with Protection Profile BSI-PP-0002-2001 at Common Criteria assurance level EAL4+
- HD65145C1 was used in the Chunghwa Telecom HICOS PKI Smart Card, which received FIPS 140-2 Validation Certificate at Level 2 from NIST, USA

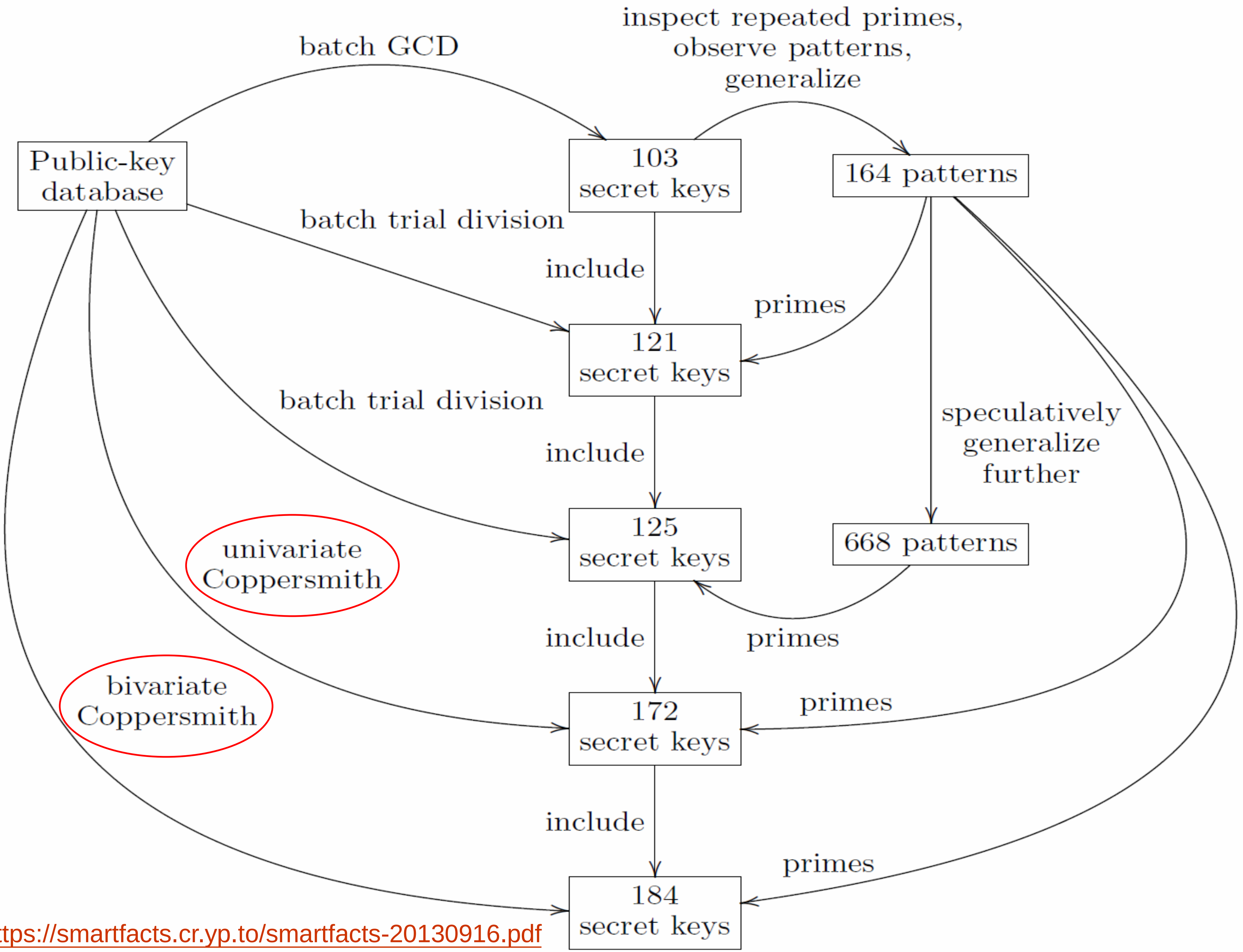
Source: Coppersmith in the wild
https://smartfacts.cr.yp.to/index.html

Citizen Certificate – Renesas

- 103 Citizen Certificate using Renesas HD65145C1 chip were broken by computing GCD of RSA public moduli
  - Some RSA moduli $N_1 = p \times q$ and $N_2 = p \times r$
  - GCD(N_1, N_2) = p, thus both N_1 and N_2 are factored
- Most frequent primes found
  - 0xc00000000000000000000000000000000000000000000000000000000000000
    000000000000000000000000000000000000000000000000000000000000002f9
  - 0xc92424922492924992494924492424922492924992494924492424922492924
    99249492449242492249292499249492449242492249292499249492449242424e5
  - 0xf6dbdb6ddb6d6db66db6b6dbb6dbdb6ddb6d6db66db6b6dbb6dbdb6ddb6d6db
    66db6b6dbb6dbdb6ddb6d6db66db6b6dbb6dbdb6ddb6d6db66db6b6dbb6dbdbc1

Source: Coppersmith in the wild
https://smartfacts.cr.yp.to/index.html

國立臺灣大學 National Taiwan University



https://smartfacts.cr.yp.to/smartfacts-20130916.pdf

Citizen Certificate – Renesas

iThome 新聞 產品評測 技術 專題 Big Data Cloud DevOps 資安 Video

自然人憑證被爆有安全漏洞！內政部：已解決

國外科技媒體報導，台灣使用的1024位元舊版自然人憑證部份使用的金鑰存在安全風險，導致駭客可能破解金鑰後冒用他人的網路身份。內政部表示，已在一兩年前就已通知這些卡片用戶更換新版卡片。

文/ 蘇文彬 | 2013-09-18 發表

讚 4.5 萬 按讚加入iThome粉絲團 讚 0 分享

中華民國內政部資訊中心
Information Center, Ministry Of The Interior

http://www.moi.gov.tw/info/news_content.aspx?sn=7771&page=0

發言人室 日期：2013-09-19

有關網路報導自然人憑證弱金鑰問題的處理情形

美國科技媒體網站(Ars Technica)日前(9月16日)刊載有關部分政府認證智慧卡之密碼瑕疵問題(Fatal crypto flaw in some government-certified smartcards makes forgery a snap)，文中引用我學者發表的論文指出，自然人憑證有弱金鑰問題，恐影響憑證的安全性。內政部就此表示，已於去(101)年7月主動更換新憑證給163張弱金鑰持卡民眾，以確保自然人憑證應用之安全。內政部表示，該文章引用之論文是緣起於我政府委託學術機構研究之結果，供有關機關自行檢視公開金鑰機制(PKI)安全強度之參考。內政部於去(101)年4月間獲悉研究團隊發現自然人憑證金鑰產製過程可能發生的問題後，即與委外技術團隊－中華電信，依研究建議方法，全面檢視所有220餘萬張自然人憑證，發現有163張卡片(原論文指出為103張)屬於弱金鑰，有被破解之可能性，已於去(101)年7月主動更換新憑證給持卡民眾使用。內政部指出，前述問題是屬於舊自然人憑證金鑰長度為1024位元所衍生(民國99年12月31日以前核發者)，民國100年以後之卡片其金鑰長度已提升為2048位元，故目前民眾使用自然人憑證之金鑰應安全無虞。鑑於電腦科技快速進步，金鑰演算法被破解之機率隨之增加，內政部表示將持續蒐集金鑰發展科技趨勢資訊，並定期檢討自然人憑證之安全有效期限，以確保自然人憑證應用於各項電子化政府網路服務之安全。

Lattice

$$L = \{\, a_1\mathbf{u_1} + a_2\mathbf{u_2} \mid a_1, a_2 \in \mathbb{Z} \,\}$$
$$= \{\, a_1\mathbf{v_1} + a_2\mathbf{v_2} \mid a_1, a_2 \in \mathbb{Z} \,\}$$ is a 2-dim **lattice**

$\{\mathbf{u_1}, \mathbf{u_2}\}$: good basis

$\{\mathbf{v_1}, \mathbf{v_2}\}$: bad basis

SVP (Shortest Vector Problem) is hard if the dimension is high

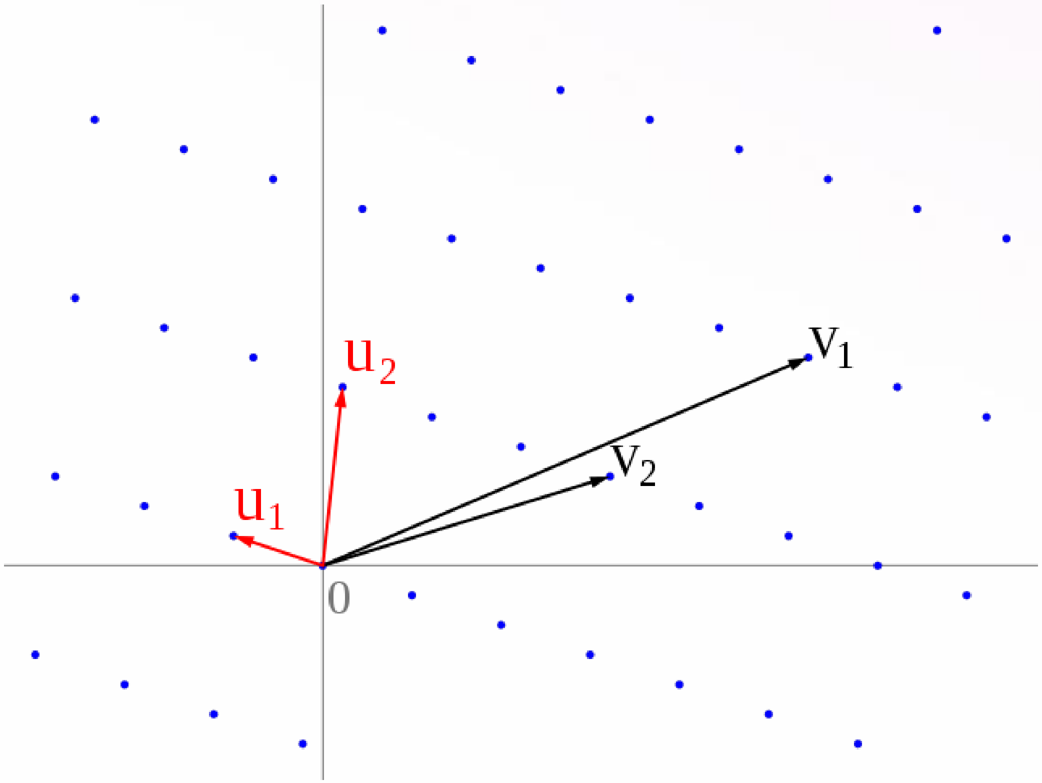


Image courtesy:
https://en.wikipedia.org/wiki/Lattice_reduction

國立臺灣大學 National Taiwan University

Coppersmith's Attack

- RSA modulus $N = p\,q$
- If $p = ax + b$ where a, b are known, and x is small enough, then x can be found by Don Coppersmith's algorithm
- Generate a lattice by known information (N, a, b), then solve SVP on the lattice

國立臺灣大學 National Taiwan University

Crypto Flaws on Chips

- EasyCard (悠遊卡) / Mifare Classic, *NXP*, 2008
- Citizen Certificate (自然人憑證), *Renesas*, 2013
  - "Coppersmith in The Wild"
- Devices around the world, *Infineon*, 2017
  - "Return of Coppersmith's Attack (ROCA)"
  - CVE-2017-15361

國立臺灣大學 National Taiwan University

ROCA

- **ROCA** – **R**eturn **o**f **C**oppersmith's **A**ttack
- The vulnerability was discovered by Slovak and Czech security researchers from the Centre for Research on Cryptography and Security at Masaryk University, Czech Republic; Enigma Bridge Ltd, Cambridge, UK; and Ca' Foscari University of Venice, Italy

國立臺灣大學 National Taiwan University

Prime Generation

- Textbook prime generation for RSA-1024
  - Choose a 512-bit random odd integer

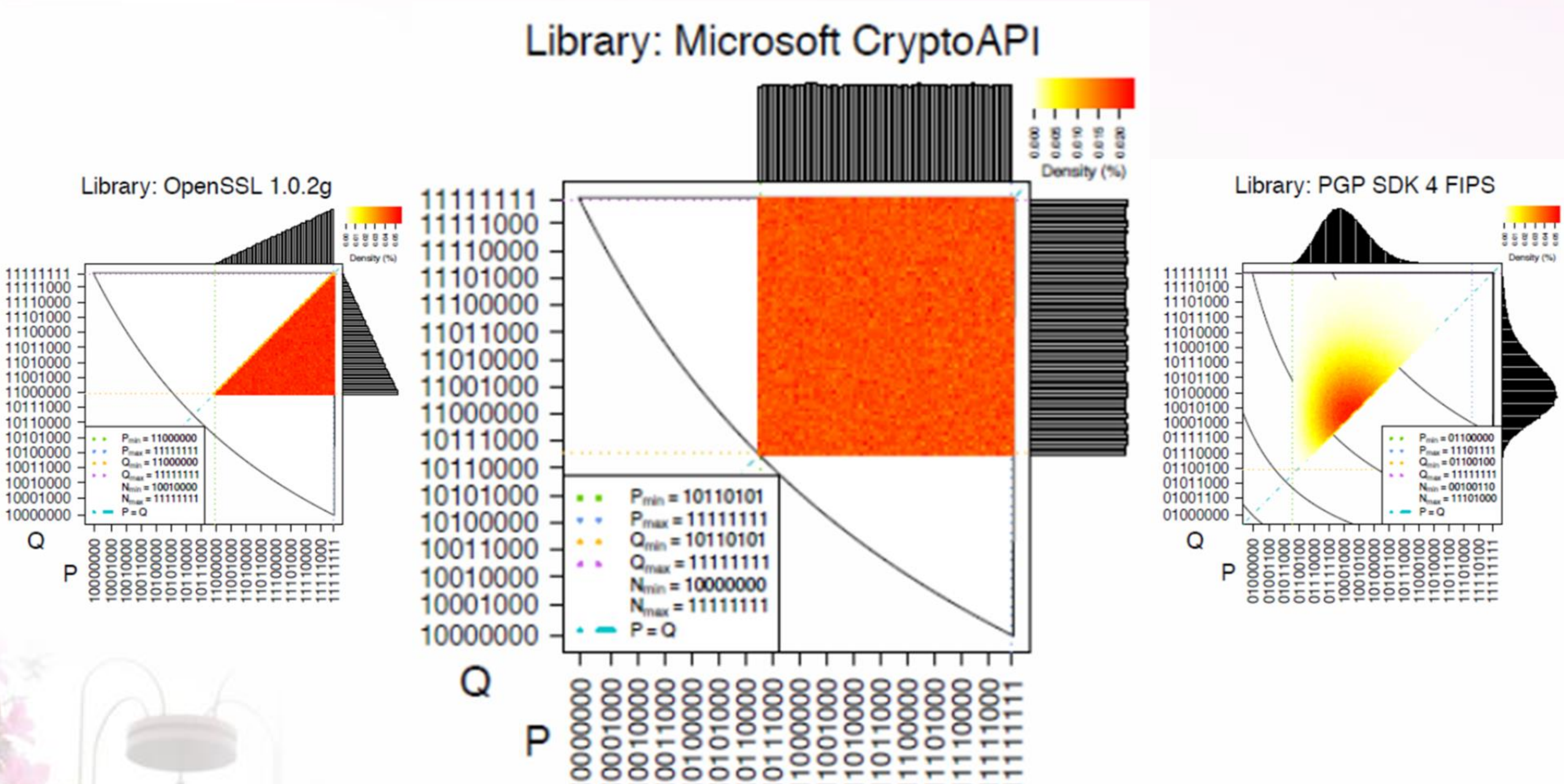
    1 …… …… …… 1

    510 random bits

  - Test divisibility for small primes: 3, 5, 7, 11, …
  - Run the Miller-Rabin test enough times
    - Reference Standard: FIPS 186-4

國立臺灣大學 National Taiwan University

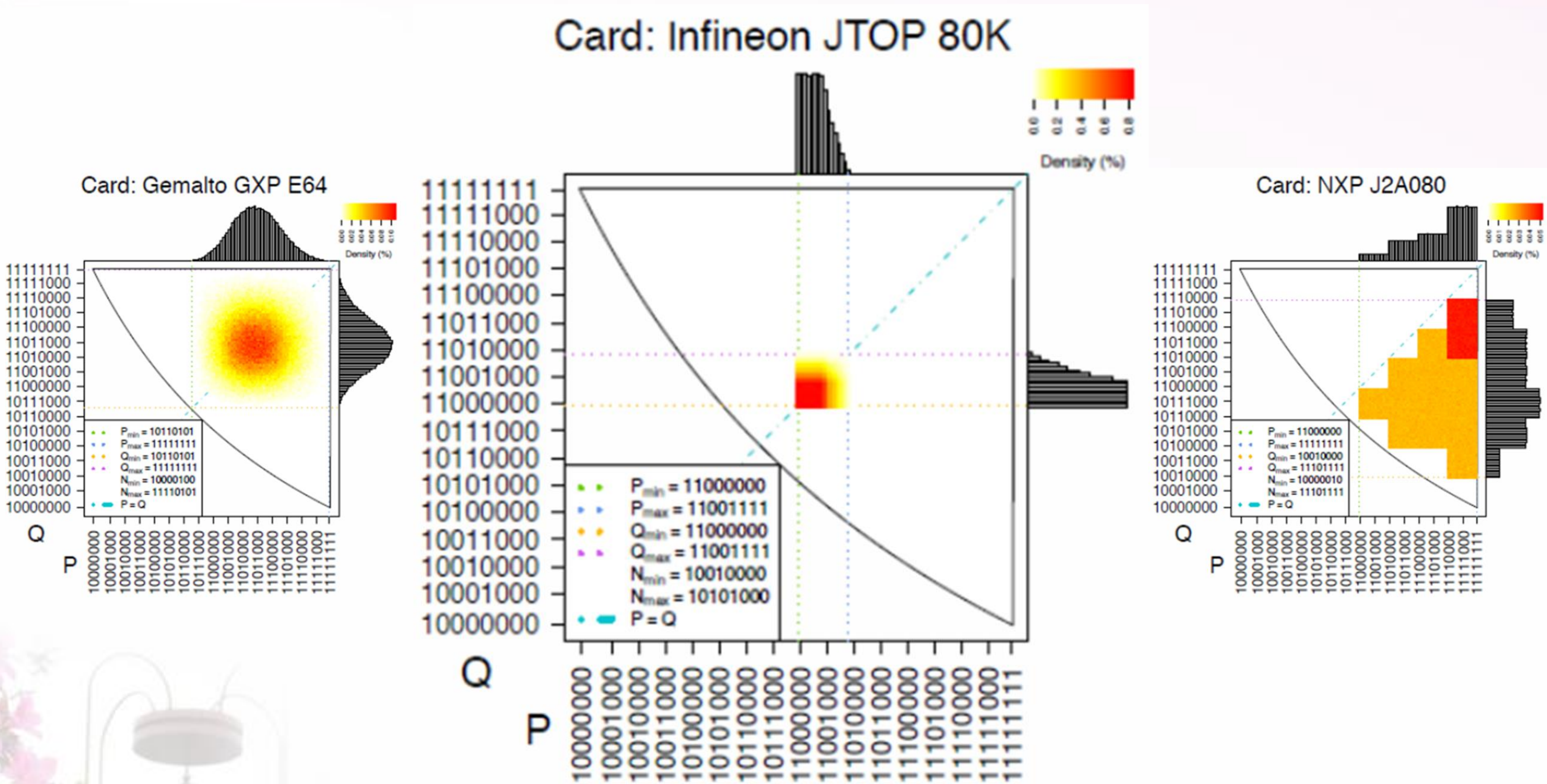
Earlier Work



https://www.usenix.org/node/197198

國立臺灣大學 National Taiwan University

Earlier Work

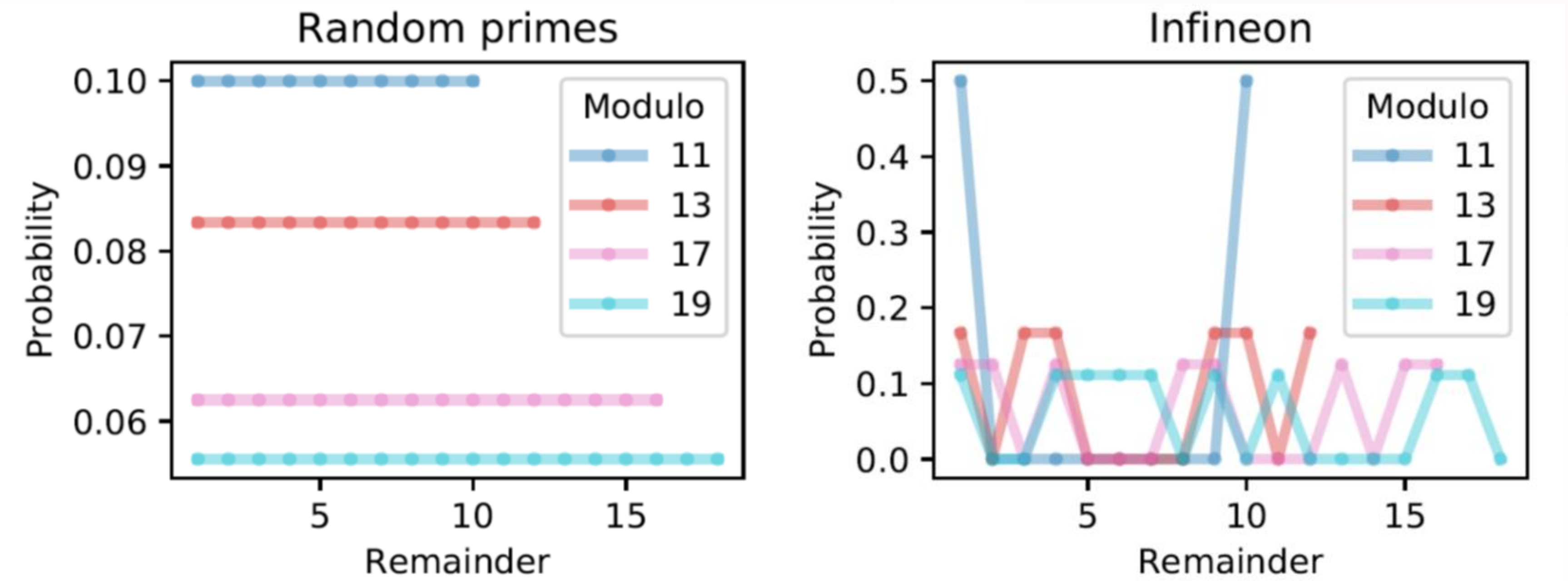


https://www.usenix.org/node/197198

國立臺灣大學 National Taiwan University

Motivation

- Distribution of RSA keys modulo small primes



https://crocs.fi.muni.cz/_media/public/papers/ccs-nemec-handout.pdf

Black-Box Attack

- The researchers had access neither to the library's source code nor to the object code
  - Stored only in the secure on-chip memory and not extractable
- The whole analysis was performed solely using RSA keys generated and exported from the Infineon's cards and tokens
- Not based on any weakness in an RNG or any additional side-channel information

https://crocs.fi.muni.cz/_media/public/papers/nemec_roca_ccs17_preprint.pdf

Infineon's Primes

- 512-bit primes (RSA-1024) are generated by

$$p = k \times M + (65537^a \bmod M)$$

  - $M = 2 \times 3 \times 5 \times \cdots \times 349 \times 353$ is fixed
    - 475 bits, the product of the first 71 primes
  - k is a 37-bit random integer
  - a is a 135-bit random integer
    - The order of the cyclic subgroup $\langle 65537 \rangle$ in the multiplicative group $\mathbb{Z}_M^*$ has 135 bits
  - Entropy: 37 + 135 = 172 bits

國立臺灣大學 National Taiwan University

Why the Formula?

$$p = k \times M + (65537^a \bmod M)$$
$$= kM + 65537^a - uM \quad \text{for some } u \in \mathbb{Z}$$

- Infineon's prime generation is much faster than the textbook method
  - For small prime $r \le 353$, $r|M$, $r \nmid 65537 \Rightarrow r \nmid p$
  - All trial divisions of p by small primes can be skipped
  - Before any primality test, the probability that the candidate p is a prime has been much larger already

國立臺灣大學 National Taiwan University

Fingerprint

$$N = \big(\underbrace{k \times M + (65537^a \bmod M)}_{p}\big) \times \big(\underbrace{l \times M + (65537^b \bmod M)}_{q}\big)$$

$$= \big(k \times l \times M + l \times (65537^a \bmod M) + k \times (65537^b \bmod M)\big) \times M$$
$$+ (65537^a \bmod M)\,(65537^b \bmod M)$$

$$\equiv 65537^{a+b} \equiv 65537^c \pmod{M}$$

- RSA modulus N is generated by Infineon's chip if and only if (almost) $c = \log_{65537} N \bmod M$ exists!

國立臺灣大學 National Taiwan University

Discrete Logarithm

- How hard is solving $N \equiv 65537^c \pmod{M}$?
  - 135-bit group order, $|\langle 65537 \rangle|$, is huge
  - However
    - $|\langle 65537 \rangle|$ divides $|\mathbb{Z}_M^*|$ by Lagrange Theorem
    - $|\mathbb{Z}_M^*| = \phi(M) = \prod_{t|M}(t-1)$ is a product of small primes, where ϕ is the Euler ϕ function
    - Hence solving $N \equiv 65537^c \pmod{M}$ by Pohlig-Hellman algorithm (divide and conquer) is pretty easy

國立臺灣大學 National Taiwan University

Naïve Factoring

$$N = p \times q = \left(k \times M + (65537^a \bmod M)\right) \times \left(l \times M + \left(65537^b \bmod M\right)\right)$$
$$\equiv 65537^{a+b} \equiv 65537^c \pmod M$$

- Once c is found, try all possible a (hence respective b is determined), and solve for k by Coppersmith's algorithm, then p is obtained
- However, it fails since there are too many possibilities ($\approx 2^{135}$) for a
- Solution: Try smaller $M'|M$ and keep primes of the same form

國立臺灣大學 National Taiwan University

Practical Factoring

$$N = p \times q = \left(k' \times M' + \left(65537^{a'} \bmod M'\right)\right) \times \left(l' \times M' + \left(65537^{b'} \bmod M'\right)\right)$$
$$\equiv 65537^{a'+b'} \equiv 65537^{c'} \pmod{M'}$$

- M' has 286 bits with $M'|M$
- The cyclic subgroup $\langle 65537 \rangle$ in $\mathbb{Z}_{M'}^*$, has 31-bit order (possibilities of a'), which is small enough
- Find c', try all possible a' (so respective b' is determined), and solve for k' (226 bits) by Coppersmith's algorithm, then p is obtained

國立臺灣大學 National Taiwan University

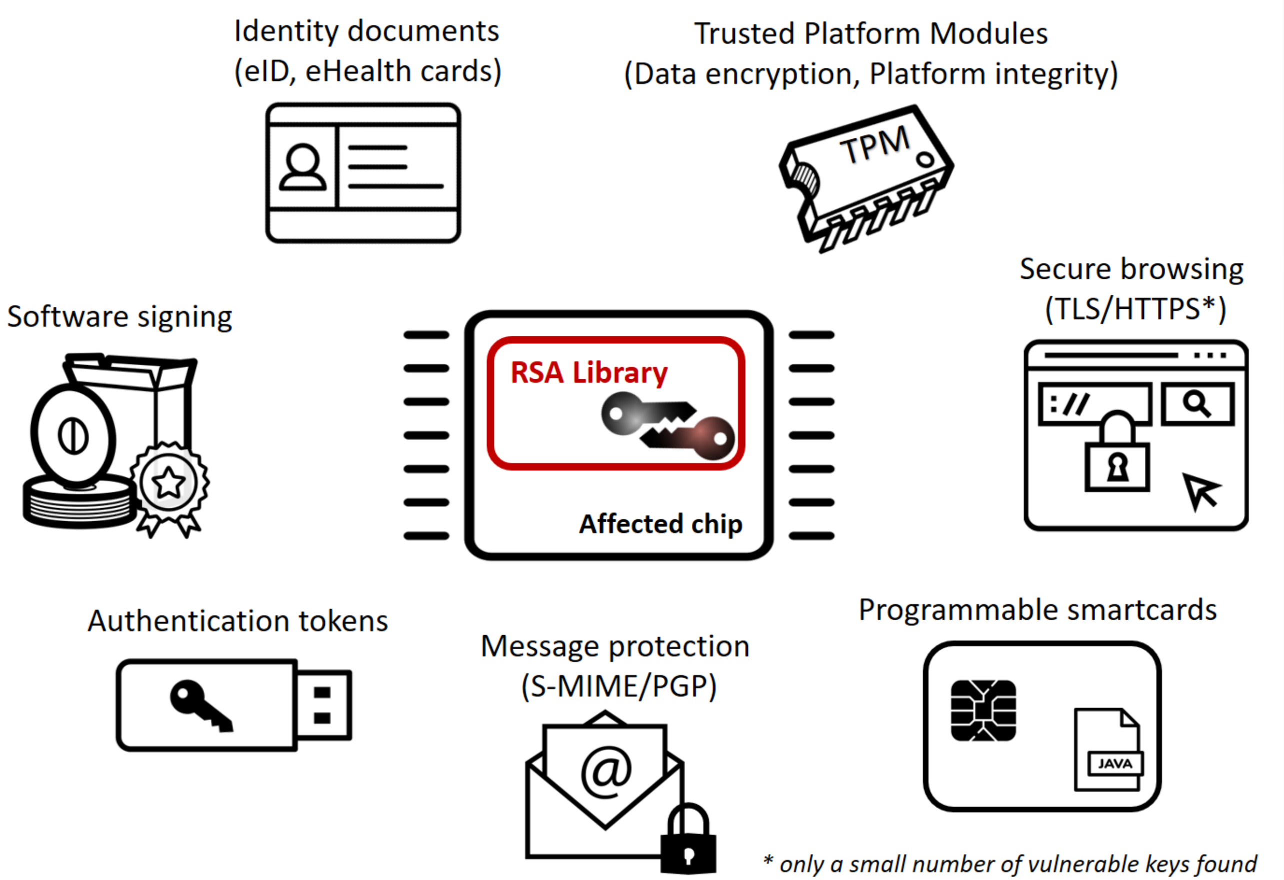
RSA 1024 & 2048

- 97.1 CPU days to factor an RSA-1024 modulus produced by Infineon chips
  - Parallelization is straightforward
  - Less than 1 day if parallelized with 100 cores
- 140.8 CPU years to factor an RSA-2048 modulus produced by Infineon chips

國立臺灣大學 National Taiwan University

Impacts

At least tens of millions devices around the world are affected



https://crocs.fi.muni.cz/public/papers/rsa_ccs17

國立臺灣大學 National Taiwan University

Morals

- Taking shortcut to enhance efficiency
  - might compromise security
  - hence very dangerous
- Secret crypto design
  - delays the discovery of flaws
  - hence impacts are increased

References

- KRACK
  - https://www.krackattacks.com
- ROCA
  - https://crocs.fi.muni.cz/public/papers/rsa_ccs17

國立臺灣大學 National Taiwan University

Thank You!