那些年的密碼學後門

講者：OAlienO

Bamboofox

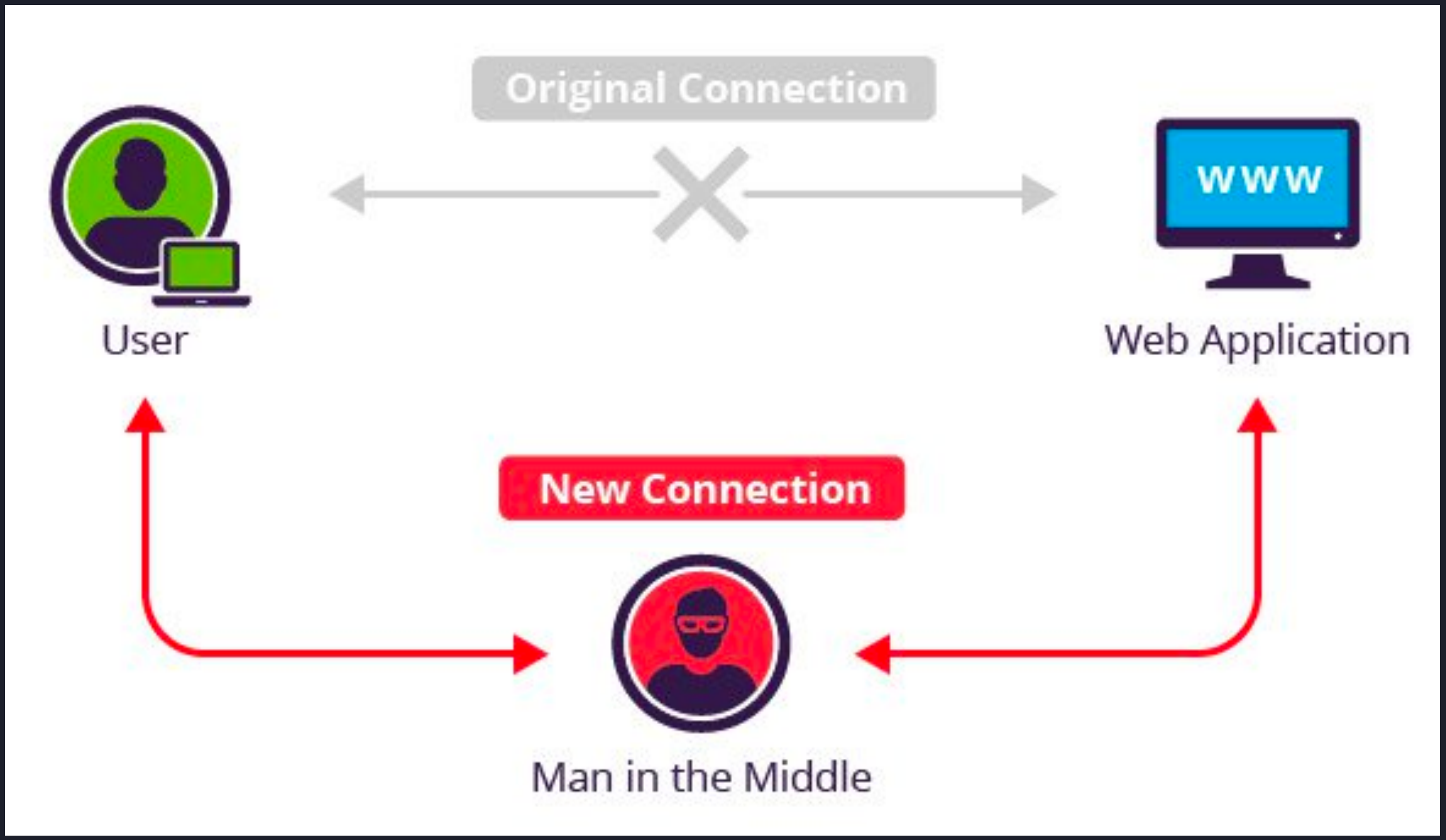
目錄

1. Cryptographic Backdoor
    - ✦ 重要性
    - ✦ 種類
2. Dual EC Backdoor
    - ✦ 介紹
    - ✦ 隨機數很重要嗎?
    - ✦ 後門原理
    - ✦ 故事時間
3. Diffie Hellman Backdoor
    - ✦ 複習時間
    - ✦ Everybody Backdoor
    - ✦ Nobody-But-Us Backdoor
4. Conclusion

Cryptographic Backdoor

Cryptographic Backdoor - 重要性

網路通訊十分依賴密碼系統
各國都想要 **監聽網路通訊** → 密碼學後門



Cryptographic Backdoor - 種類

Everybody Backdoors :

所有人都可以進來的後門，與其說後門，不如說是故意設置的漏洞

Nobody-But-Us (NOBUS) Backdoors

只有擁有金鑰的人才能用的後門，真正的後門

Dual EC Backdoor

Dual EC - 介紹

Dual EC 是一個偽隨機數產生器 (pseudorandom number generator)
剛公布 Dual EC 的時候他就有許多問題

1. **比其他的 PRNG 慢**
2. **產生的隨機數沒有那麼隨機 (biased)**
3. **可能有後門存在這個 PRNG**

Dual EC - 隨機數很重要嗎？

1. DSA - private key
2. AES - iv, key
3. RSA - p, q
4. …

許多的密碼系統都需要隨機數
當我們能預測這些隨機數，差不多就等同於我們可以破解他

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

Dual EC 有兩個版本：

Dual EC 2006

Dual EC 2007

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

Dual EC 2006

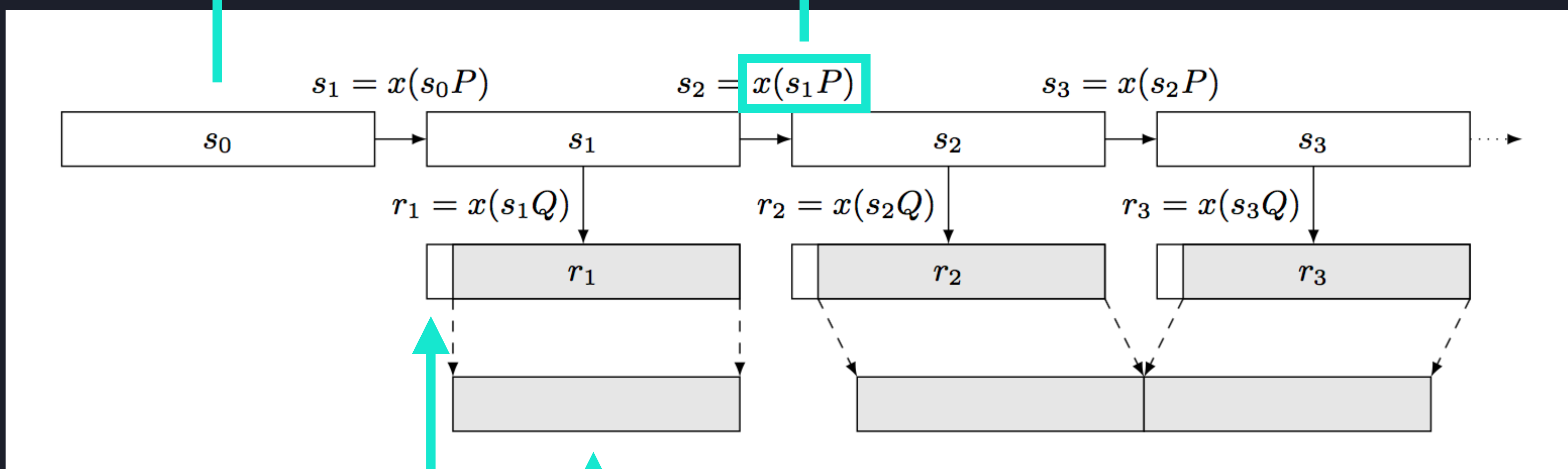
Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

P, Q 是在 Elliptic Curve 上的點

256 bits 整數

不可逆函式



丟掉 16 bits

輸出

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

橢圓曲線 (Elliptic Curve) ?
就是滿足下面方程式的一堆點

$$E = \{(x, y) \mid y^2 = x^3 + ax + b\} \text{ where } 4a^3 + 27b^2 \neq 0$$

$$x, y, a, b \in \mathbb{R} \text{ or } \mathbb{Q} \text{ or } \mathbb{C} \text{ or } \mathbb{Z}_p$$

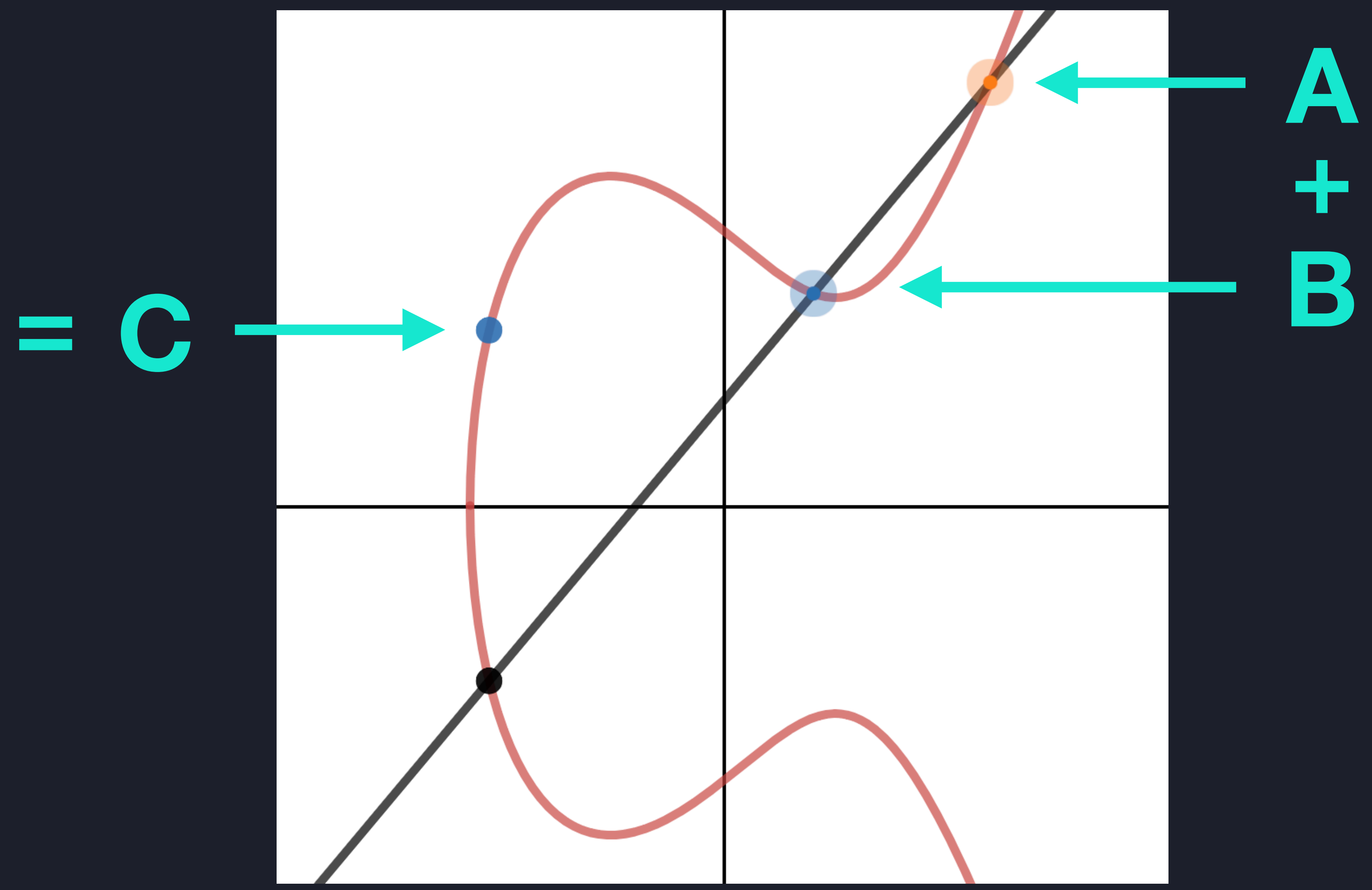
在密碼學我們是用這個

有了一堆點形成的集合
再定義一個加法運算
我們就得到了一個群

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

兩個在 Elliptic Curve 上的點怎麼加法？
切線交點對 x 軸鏡射



Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

我們的不可逆函式就是一個

ECDLP (Elliptic Curve Discrete Logarithm Problem)

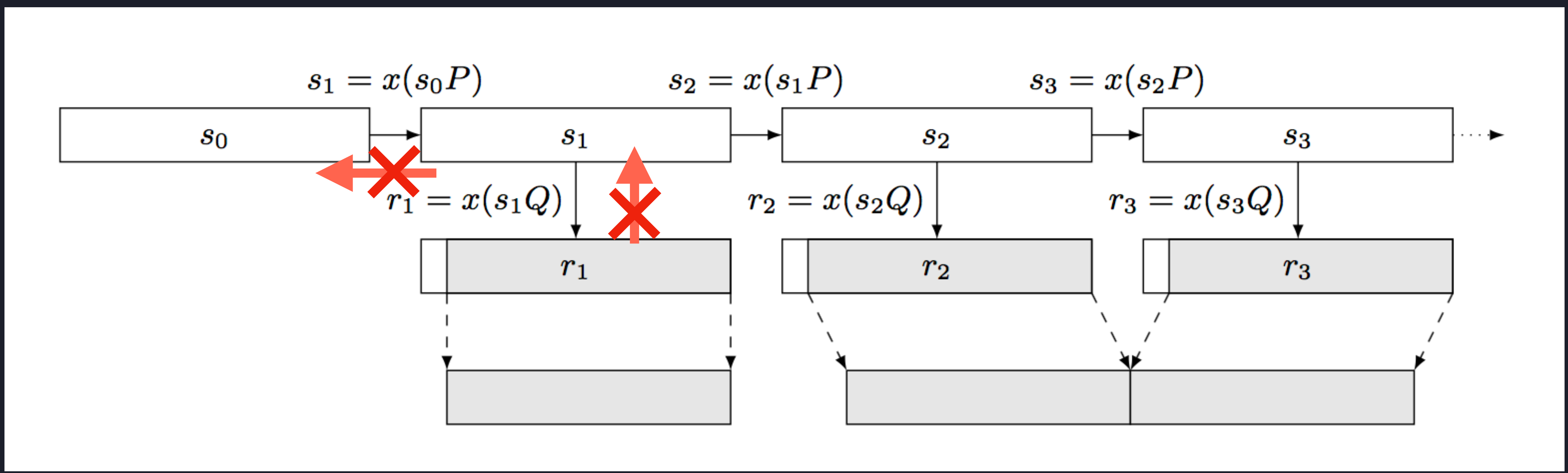
$$\text{給 } sP = \underbrace{P + P + \cdots + P}_{\text{s times}} \text{ 求 } s\,?$$

這是個非常難的問題，所以可以把他當作不可逆函式

$x(sP)$ 就是 sP 這個點的 x 座標

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf



有了不可逆函式

我們沒辦法從輸出 r 反推內部狀態 s

也就沒辦法從內部狀態 s 往下預測接下來的輸出

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

It sounds perfect
What could possibly go wrong ?

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

如果攻擊者知道 d 使得 $P = dQ$

將 r_1 帶進橢圓曲線式子找回 y 座標 y_{r_1}

$$
\begin{aligned}
(r_1, y_{r_1}) &= s_1 Q \\
d(r_1, y_{r_1}) &= s_1 d Q \\
d(r_1, y_{r_1}) &= s_1 P
\end{aligned}
$$

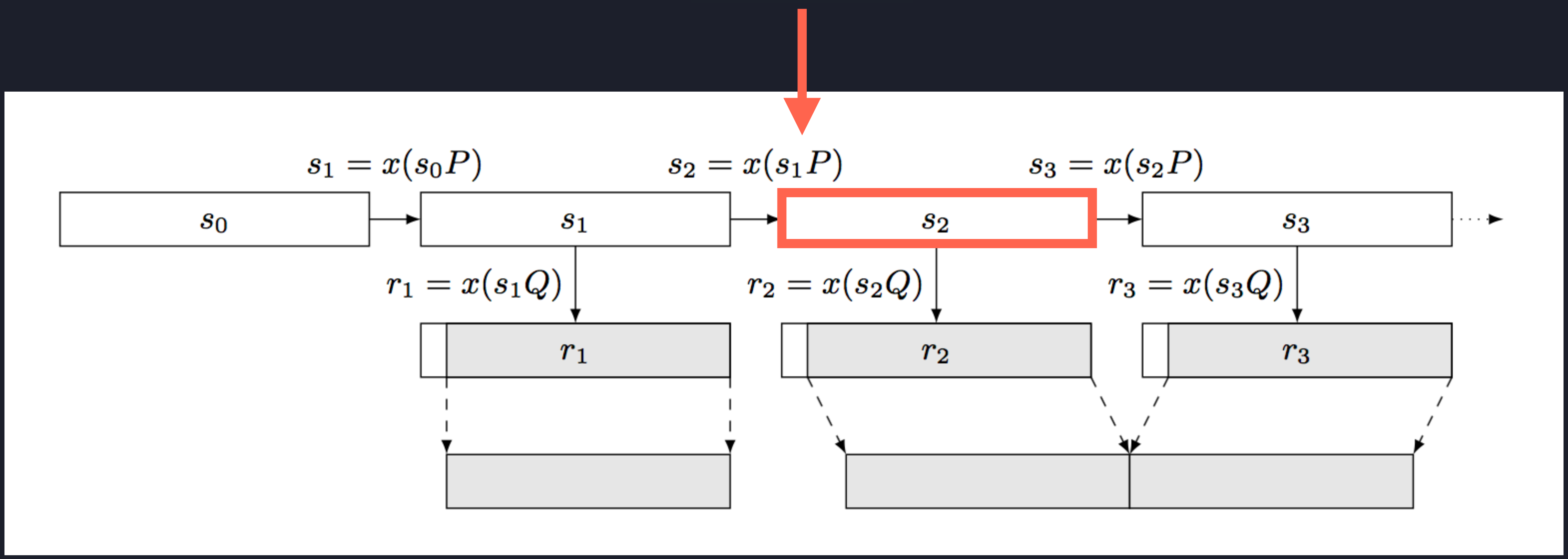
那丟掉的 16 bits 怎麼辦？

直接暴力嘗試 $2^{16} = 65536$

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

知道 $s_1 P$ 得天下

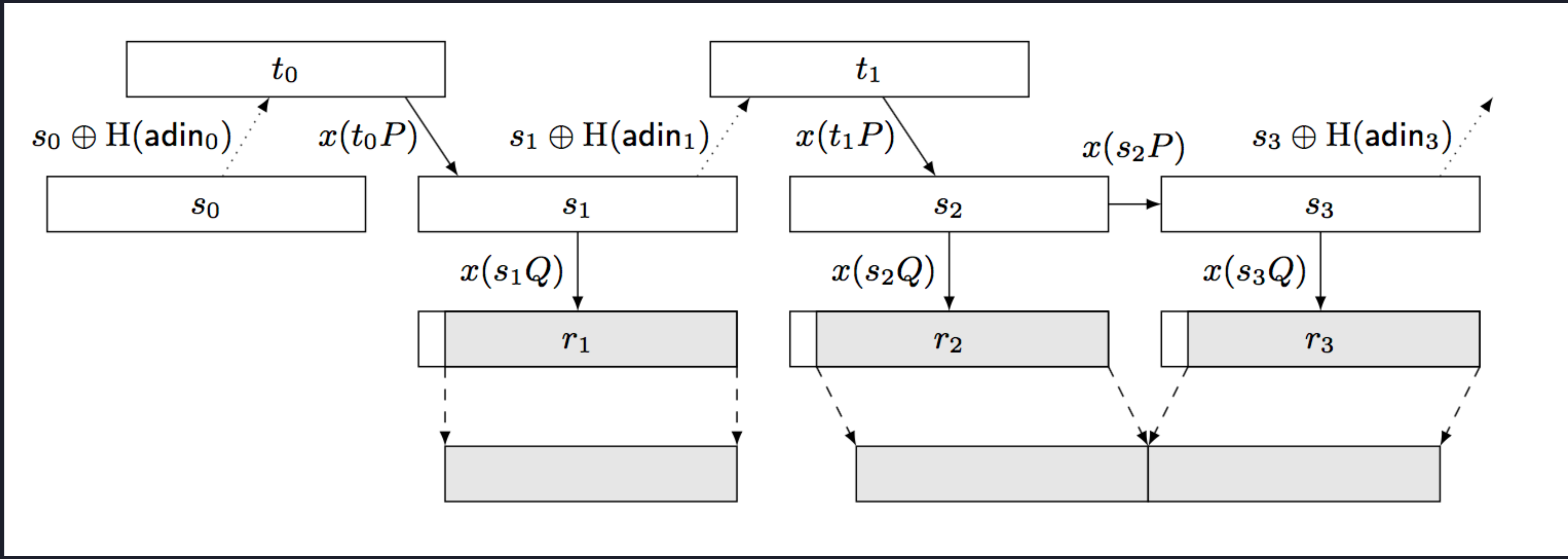


Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

使用者可以選擇要不要用

他其實還有一個功能
可以在輸出完將目前的內部狀態 xor 一個 additional input
但是這個功能會損壞後門，讓後門不好用

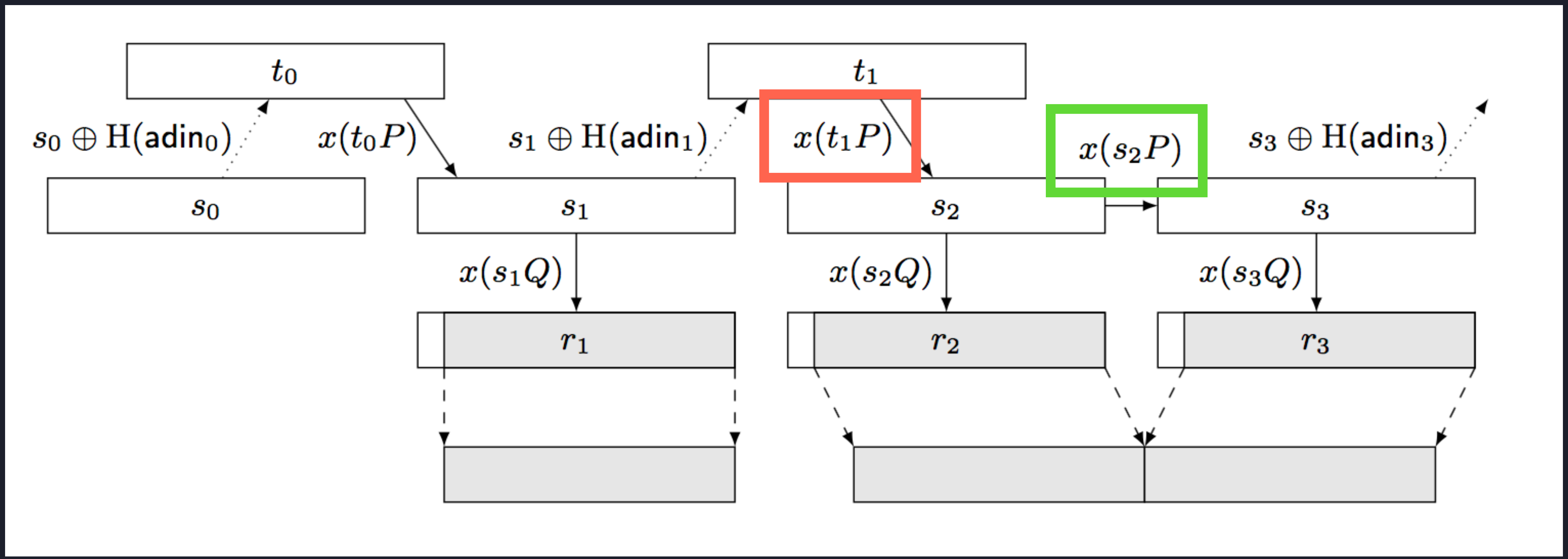


Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

我們沒辦法從 s_1P 求出 $(s_1 \oplus H(adin_1))P$ ⟶ 無法還原內部結構 s2

要求的輸出超過兩個區塊 s_2P 不受影響 ⟶ 還原內部結構 s3



Dual EC - 後門原理

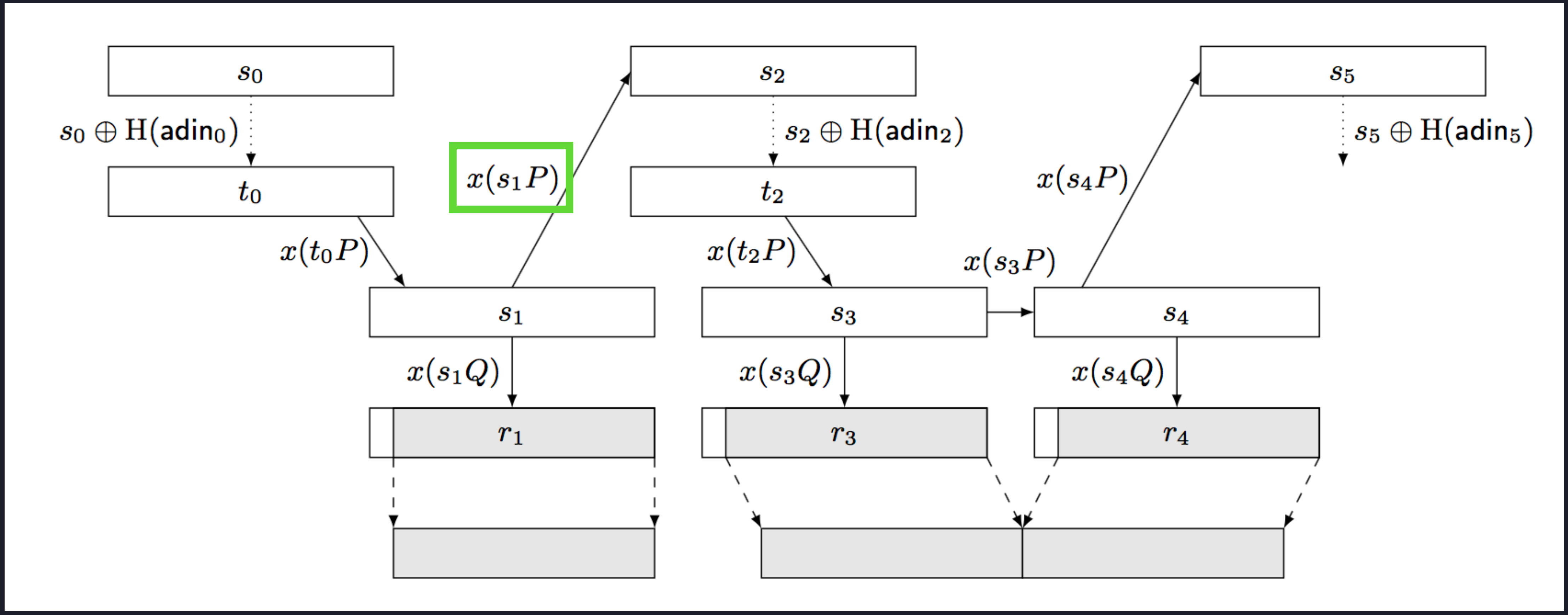
https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

Dual EC 2007

Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

Dual EC 2007 修好了後門
我們同樣可以從 s_1P 推出 s_2 以及接下來的狀態
但是還是需要猜 additional input



Dual EC - 後門原理

https://projectbullrun.org/dual-ec/documents/dual-ec-20150731.pdf

所以真的有後門嗎？

NIST SP 800-90 裡面完全沒提到 P, Q 從哪裡來的

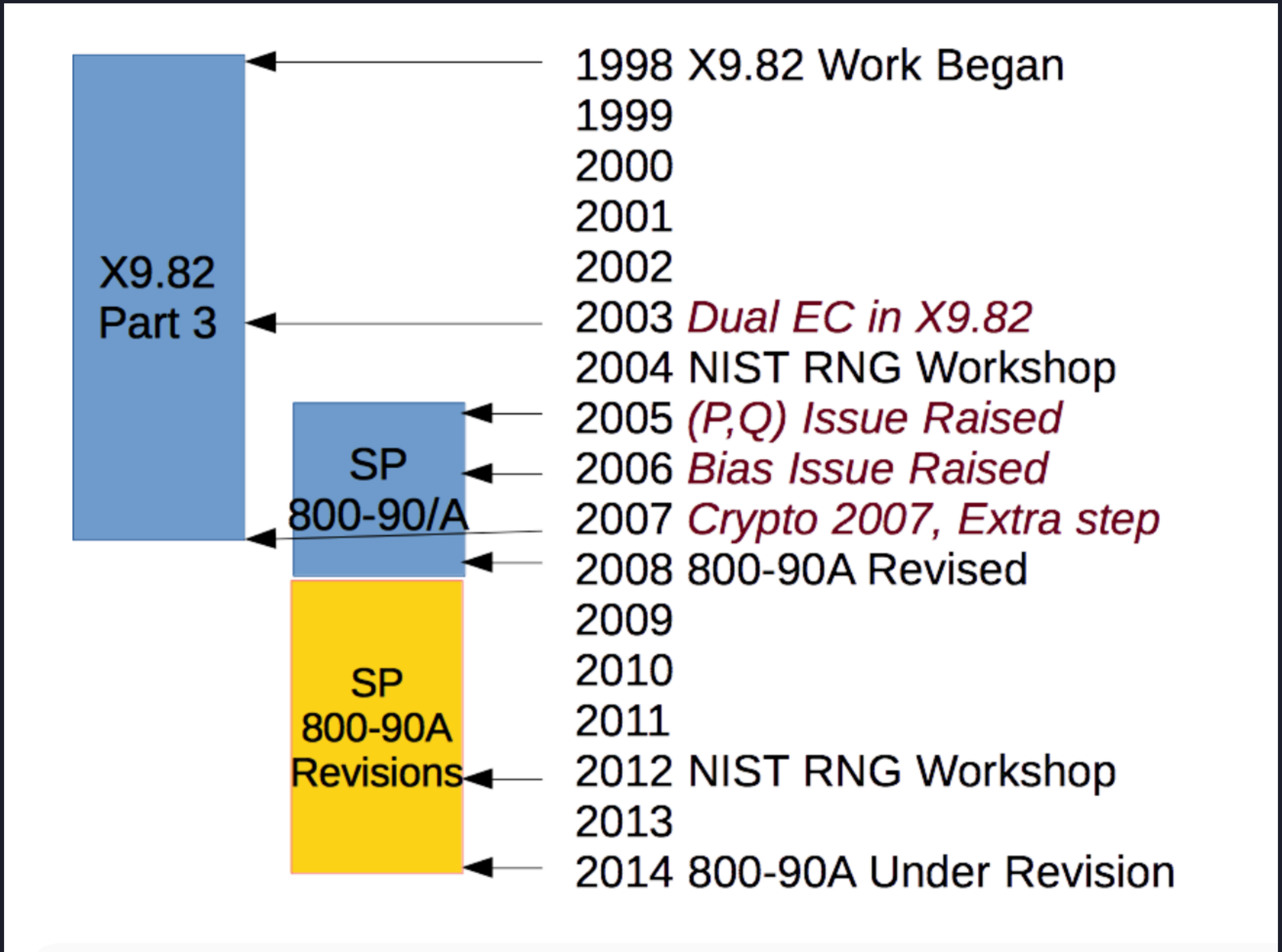
$P = dQ$ 求 d 是個 ECDLP

我們知道可能有後門但不能證明有

直到 Edward Snowden 洩漏出 NSA 的文件 XD

Dual EC - 故事時間

https://csrc.nist.gov/csrc/media/projects/crypto-standards-development-process/documents/dualec_in_x982_and_sp800-90.pdf



Dual EC - 故事時間

https://eprint.iacr.org/2006/190.pdf

2006 / 05 / 29

論文提出 Dual EC 的輸出沒有很隨機

Cryptanalysis of the Dual Elliptic Curve Pseudorandom Generator

Berry Schoenmakers and Andrey Sidorenko
Dept. of Mathematics and Computer Science, TU Eindhoven,
P.O. Box 513, 5600 MB Eindhoven, The Netherlands.
berry@win.tue.nl, a.sidorenko@tue.nl

29 May 2006

3 The Distinguishing Attack on the DEC PRG

Dual EC - 故事時間

http://rump2007.cr.yp.to/15-shumow.pdf

2007 / 08

Crypto 2007 rump session

Microsoft 人員提出 Dual EC 可能有後門

On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng

Dan Shumow

Niels Ferguson

Microsoft

Dual EC - 故事時間

https://www.wired.com/2007/11/securitymatters-1115/

2007 / 11 / 15

一篇部落格談論 Dual EC 是不是真的有後門

BRUCE SCHNEIER BUSINESS 11.15.07 12:00 PM

DID NSA PUT A SECRET BACKDOOR IN NEW ENCRYPTION STANDARD?

Dual EC - 故事時間

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation/validation-list/drbg

2008 / 07 / 03

RSA BSAFE 採用 Dual EC

RSA BSAFE Crypto-C Micro Edition (ME) 3.0 *RSA BSAFE® Crypto-C ME software is designed to help protect sensitive data as it is stored using strong encryption techniques to provide a persistent level of protection. The software supports a wide range of industry standard encryption algorithms offering developers the flexibility to choose the appropriate option to meet their requirements.*	7/3/2008	~~*Dual EC:*~~ ~~*P-256 Modes: SHA-1, SHA-224, SHA-256, SHA-384, SHA-512*~~ ~~*P-384 Modes: SHA-224, SHA-256, SHA-384, SHA-512*~~ ~~*P-521 Modes: SHA-256, SHA-384, SHA-512*~~ ~~*Prerequisite: SHS #807, ECDSA #92*~~

Dual EC - 故事時間

https://csrc.nist.gov/projects/cryptographic-algorithm-validation-program/validation/validation-list/drbg

2009 / 09 / 30

Windows 7 採用 Dual EC

Windows 7 CNG algorithms 1.0 *The Microsoft Windows Cryptographic Primitives Library is a general purpose, software-based, cryptographic module which can be dynamically linked into applications by developers to permit the use of FIPS 140-2 Level 1 compliant cryptography.*	9/30/2009	~~Dual EC:~~ ~~P-256 Modes: SHA-256~~ ~~Prerequisite: SHS #1081~~

Dual EC - 故事時間

https://en.wikipedia.org/wiki/File:Classification_guide_for_Project_BULLRUN.pdf

2013

Snowden leaks - Project BULLRUN
驗證後門真的存在

TOP SECRET//SI//REL TO USA, FVEY

CLASSIFICATION GUIDE TITLE/NUMBER: (U//FOUO) PROJECT BULLRUN/2-16

PUBLICATION DATE: 16 June 2010

OFFICE OF ORIGIN: (U) Cryptanalysis and Exploitation Services

POC: (U) Cryptanalysis and Exploitation Services (CES) Classification Advisory Officer

PHONE: [redacted]

ORIGINAL CLASSIFICATION AUTHORITY: [redacted]

1. (TS//SI//REL) Project BULLRUN deals with NSA's abilities to defeat the encryption used in specific network communication technologies. BULLRUN involves multiple

Dual EC - 故事時間

https://www.theverge.com/2013/12/20/5231006/nsa-paid-10-million-for-a-back-door-into-rsa-encryption-according-to

2013 / 12 / 20

NSA 給 RSA 一千萬美金
將 Dual EC 設為 BSAFE 的 預設 隨機產生器

NSA paid $10 million to put its backdoor in RSA encryption, according to Reuters report

By Russell Brandom | @russellbrandom | Dec 20, 2013, 4:54pm EST

Dual EC - 故事時間

https://www.cbronline.com/news/iso-nsa

2018 / 04 / 27

ISO 拒絕 將
NSA 設計的 Simon & Speck 列為標準

NSA: Our Crypto Is Good. ISO: No Thanks Though

ED TARGETT EDITOR

+ INCREASE / DECREASE TEXT SIZE −

27TH APRIL 2018

Diffie Hellman Backdoor

Diffie Hellman Backdoor - 複習

群 (Group)

一個群 G 就是帶有一個運算元 $\bullet$ 的集合

並且具備以下四種性質

1. 封閉性 (Closure) : $\forall a, b \in G : a \bullet b \in G$
2. 結合律 (Associativity) : $\forall a, b, c \in G : (a \bullet b) \bullet c = a \bullet (b \bullet c)$
3. 存在單位元素 (Identity element) : $\exists e \in G : \forall g \in G : e \bullet g = g \bullet e = g$
4. 任一元素有一反元素 (Inverse element) : $\forall g \in G : \exists g^{-1} \in G : g^{-1} \bullet g = g \bullet g^{-1} = e$

簡而言之 : 群就是 <u>一個集合</u> + <u>一個運算元</u> 滿足 <u>一些條件</u>

Diffie Hellman Backdoor - 複習

Order

order of a $\boxed{\text{group}}$ G 是指該群 G 的元素個數

order of an $\boxed{\text{element}}$ a in a group 是指最小的正整數 m 滿足 $a^m = e$ (e 是該群的單位元素)

Diffie Hellman Backdoor - 複習

Smooth Number

一個 smooth 的正整數的質因數都很小

一個 B-smooth 的正整數的質因數都不大於 B

Diffie Hellman Backdoor - 複習

什麼是 Diffie Hellman？

Diffie-Hellman Key Exchange 可以在雙方沒有任何共通資訊的情況下，在不安全的通道中共享祕密

假設我們有一個質數 p 和一個整數 g

Alice 和 Bob 想要共享祕密

1. Alice 隨機產生 a，Bob 隨機產生 b
2. Alice 計算 $g^a \bmod p$，傳送給 Bob
3. Bob 計算 $g^b \bmod p$，傳送給 Alice
4. Alice 計算 $(g^b \bmod p)^a \bmod p = g^{ab} \bmod p$
5. Bob 計算 $(g^a \bmod p)^b \bmod p = g^{ab} \bmod p$
6. Alice 和 Bob 共享祕密 $g^{ab} \bmod p$

Diffie-Hellman Key Exchange 能防止**竊聽**但不能防止**中間人攻擊**

Diffie Hellman Backdoor - 複習

Discrete Logarithm Problem (DLP)

Diffie Hellman 破解的困難點在於 Discrete Logarithm Problem 沒有有效的方式求解

Discrete Logarithm Problem :

給一質數 p，一個生成元 $\alpha \in \mathbb{Z}_p^*$，一個元素 $\beta \in \mathbb{Z}_p^*$ ($\mathbb{Z}_p^*$ has order n)

求 x 滿足 $\alpha^x \equiv \beta \pmod{p}$

Diffie Hellman Backdoor - 複習

Pollard's Rho Algorithm

求 x 滿足 $\alpha^x \equiv \beta \pmod p$

用 Floyd's Cycle Finding Algorithm 尋找 a, b, A, B 滿足 $\alpha^a \beta^b \equiv \alpha^A \beta^B \pmod p$

$$\alpha^{bx+a} \equiv \alpha^{Bx+A} \pmod p$$

$$bx + a \equiv Bx + A \pmod n$$

$$x = (B - b)^{-1}(a - A) \mod n$$

用來解 Discrete Logarithm Problem

時間複雜度：$O(\sqrt{n})$

Diffie Hellman Backdoor - 複習

Pohlig Hellman Algorithm

求 x 滿足 $\alpha^x \equiv \beta \pmod{p}$

$$p - 1 = p_1^{e_1} \cdot p_2^{e_2} \cdots p_r^{e_r}$$

先求 $x_i = x \mod p_i^{e_i}$，再用中國剩餘定理組回 x

用來解 Discrete Logarithm Problem

使用條件 : 當 p - 1 是 smooth number

時間複雜度 : $O(\sqrt{p_i})$

Diffie Hellman Backdoor - Everybody

https://eprint.iacr.org/2016/644.pdf

Everybody Backdoors :

1. p - 1 選 B-smooth 的數，讓我們可以用 Pohlig-Hellman 解 DLP
2. 選一個 order 很小的 element 當 g，讓我們可以用 Pollard’s Rho 解 DLP

$$\varphi(p) = p - 1 = \boxed{p_1} \times \cdots \times p_k$$

order

$$y = g^x \pmod{p}$$

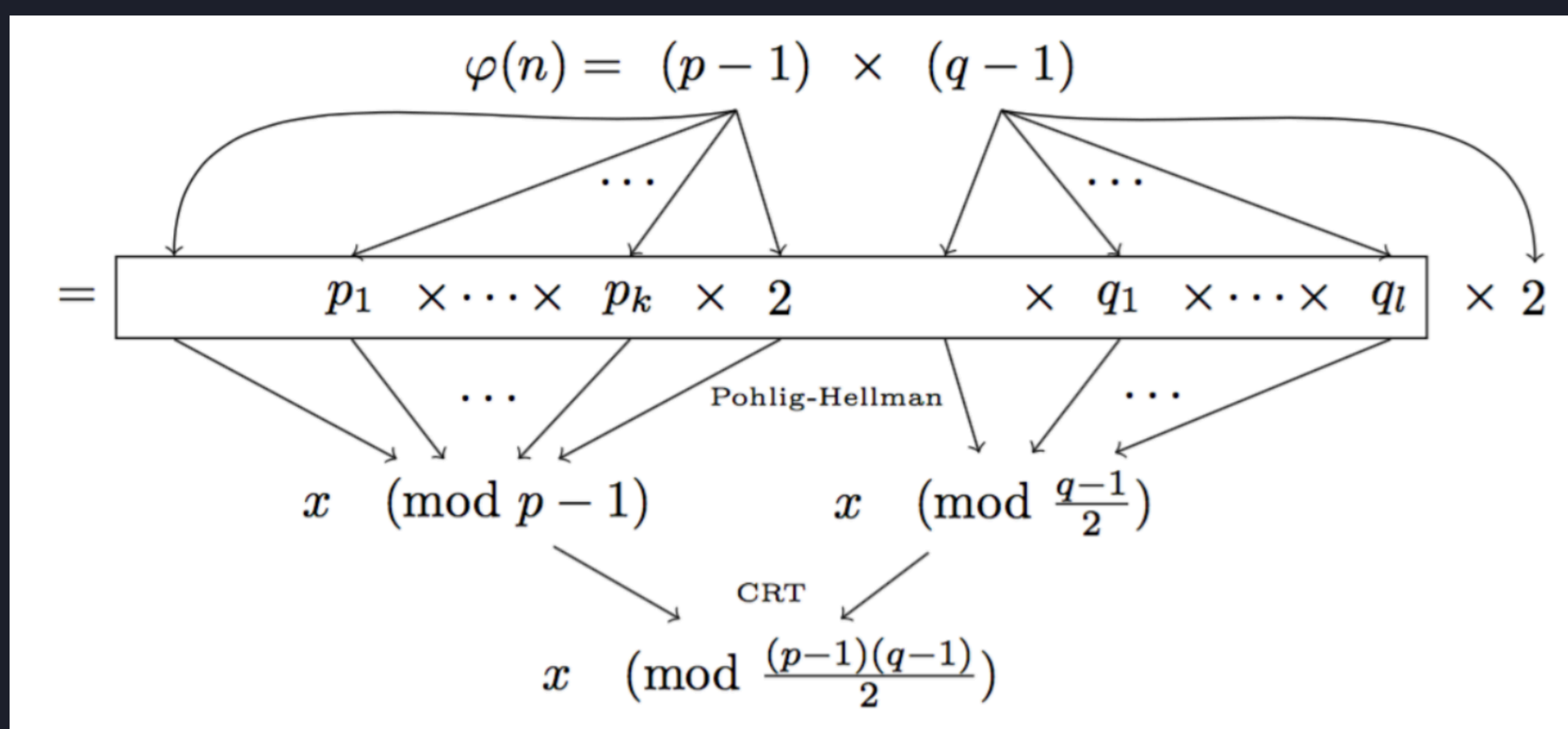
Diffie Hellman Backdoor - NOBUS

https://eprint.iacr.org/2016/644.pdf

NOBUS Backdoors :

選 $n = pq$，使得 (p - 1) 和 (q - 1) 都是 B-smooth

這樣只有能分解 $n = pq$ 的人可以用 $(p-1), (q-1)$ 的小質數們做 Pohlig Hellman



Diffie Hellman Backdoor - NOBUS

https://eprint.iacr.org/2016/644.pdf

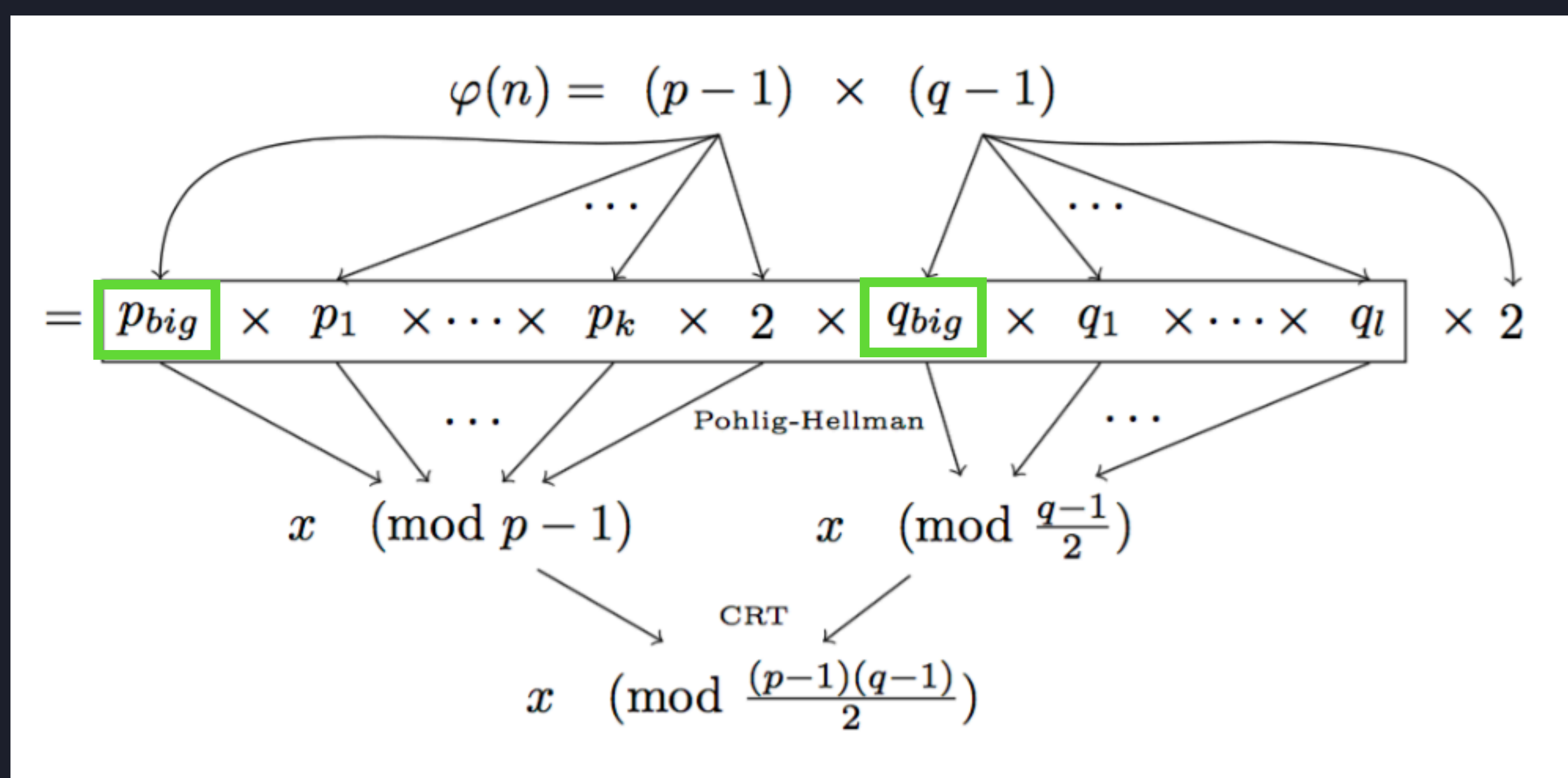
問題來了：

當 (p - 1) 和 (q - 1) 都是 B-smooth 的話
可以直接用 Pollard's p - 1 Algorithm 分解 n
這樣所有人都可以用我們的後門 (NOT GOOD)

Diffie Hellman Backdoor - NOBUS

https://eprint.iacr.org/2016/644.pdf

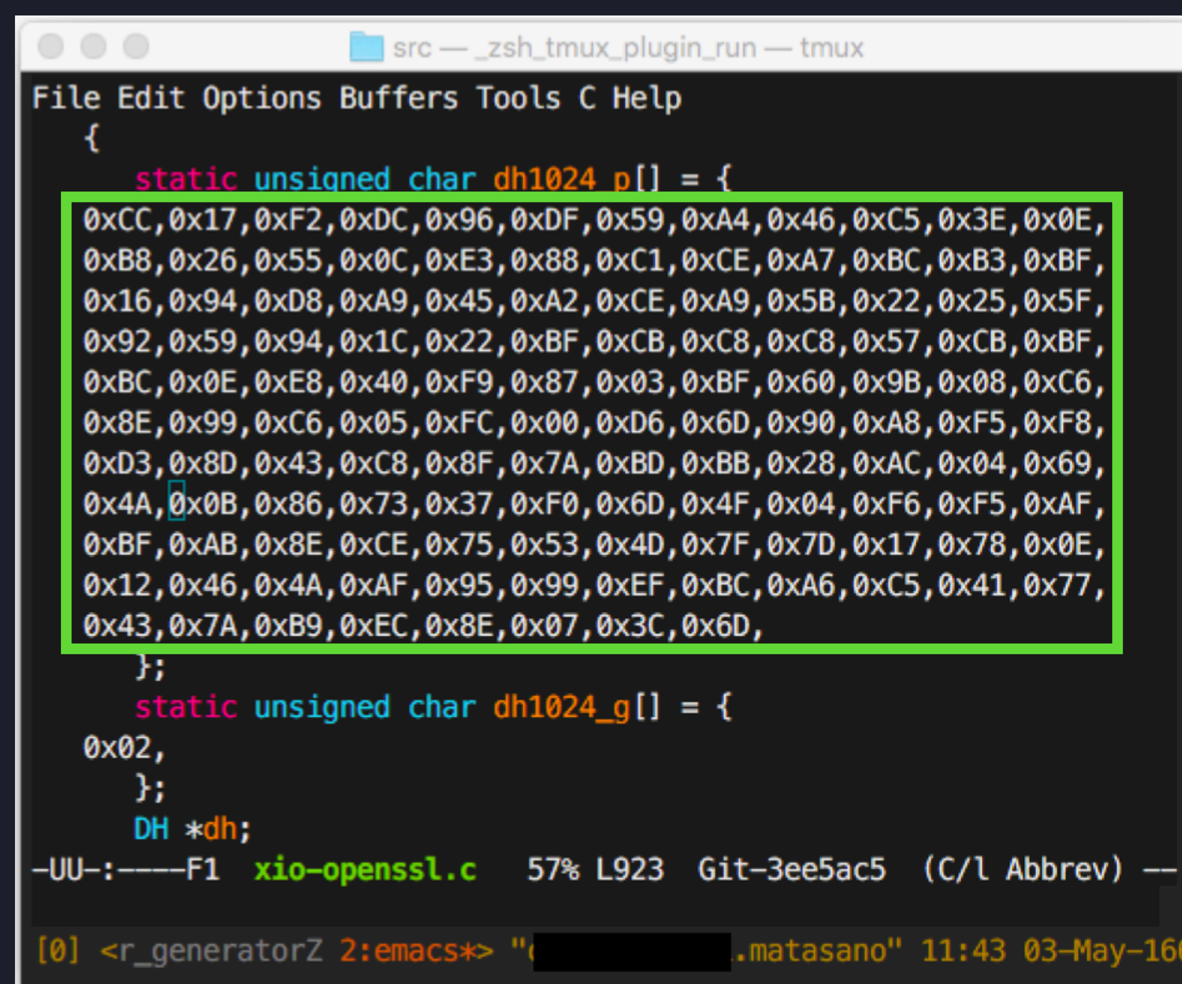
引入 p_{big} 和 q_{big} 兩個相對較大的質數
用來抵擋 Pollard's p - 1 Algorithm



Diffie Hellman Backdoor - NOBUS

https://eprint.iacr.org/2016/644.pdf

不像一般的惡意程式後門
使用這個後門時，我們只需要把 **常數** 換掉
完全看不出來我們在裝後門 XD



Diffie Hellman Backdoor - 防禦

https://eprint.iacr.org/2016/644.pdf

針對這個後門的防禦很簡單
就是確保參數 p 真的是一個質數
如果允許 p 是合數的話
還是很難分辨後門和不是後門

Conclusion

Conclusion

這次介紹了兩個密碼學後門
Dual EC Backdoor 和 Diffie Hellman Backdoor

可以看出密碼學後門的防護相較一般的後門困難
1. 沒有 general 的防護方式
2. 需要單獨作分析來防禦
3. 有些甚至無法證明有沒有被塞後門
4. 使用其他人設計的密碼系統就會有風險

THANKS