RSA后门及应对方案

主要内容

- 事件背景
- RSA后门问题
- 事件联想
- 随机数生成器
- 致谢

事件背景

- 斯诺登“棱镜门”事件
- 美国国安局(NSA)曾与业内影响力巨大的电脑安全公司RSA达成了一个价格高达1000万美元的秘密协议，NSA要求RSA在安全软件中使用NSA设计的一个方程式
- 被染指产品（Bsafe）
  - BSafe安全软件被业界广泛使用包括电子商贸、银行、政府机构、电信、宇航业、大学等

RSA后门问题

- RSA后门不是指RSA算法的漏洞，而是随机数生成器

- NIST的SP800-90随机数生成器推荐标准
  - Hash_DRBG
  - HMAC_DRBG
  - CRT_DRBG
  - DUAL_EC_DRBG (后门)

RSA后门问题

- 随机数生成器
  - 随机数被广泛用于密钥产生、初始化向量、时间戳、认证挑战码、密钥协商、大素数产生等等方面，因此随机数在密码学中的具有十分重要的地位

- 随机数分类
  - 确定性随机数（伪随机数）
  - 非确定行随机数（真随机数）

DUAL_EC_DRBG属于确定性随机数生成器

RSA后门问题

- DUAL_EC_DRBG

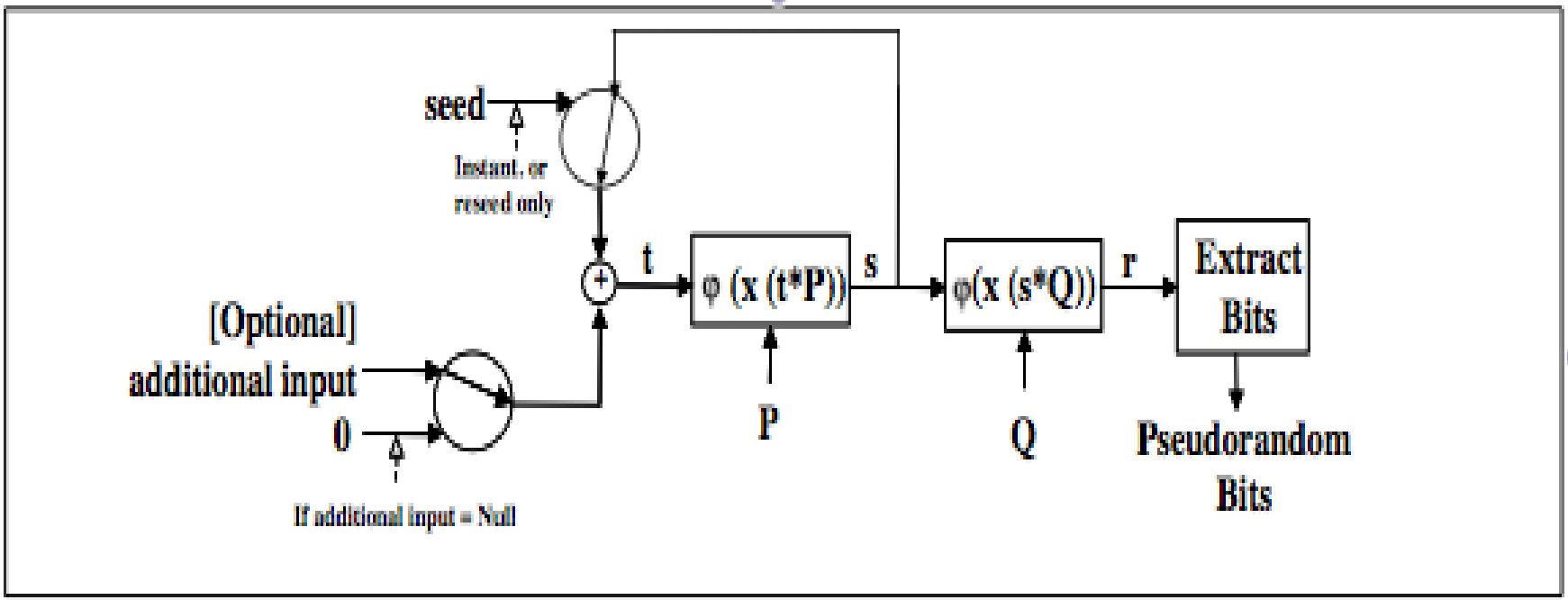


Figure 13: Dual_EC_DRBG

RSA后门问题

- 后门条件：
  - ①additional_input为空
  - ②攻击者知道Q=aP中的a
  - ③能得到一个r_i值

- Crypto 2007会议上，Dan Shumow 和Niel Fergusonsu
- 作了一个报告宣布NISTSP800-90 中的 Dual_EC_DRBG
- 存在可能的后门。攻击者者可以利用它来预测该确定性随
- 机数产生后续的比特流，从而破坏了“不可预测”的性质
- http://rump2007.cr.yp.to/15-shumow.pdf

RSA后门问题

- 具体如下：

$$t_i = s_{i-1} \oplus additional\_input$$
$$s_i = \varphi(x(t_i * P))$$
$$r_i = \varphi(x(s_i * Q))$$

其中函数 $x(P)$ 是取得点 P 的 x 坐标。$\varphi(x)$ 函数是将 x 转化为合适的正整数，P 和 Q 均是椭圆曲线上的基点，且有 $Q = aP$ 。

我们考虑一种情况，如果条件①*additional_input* 为空值。那么有：

$$s_i = \varphi(x(s_{i-1} * P))$$
$$r_i = \varphi(x(s_i * Q))$$

另外如果条件②攻击者知道$Q = aP$中的a，并且条件③能得到一个r_i值，那么他就可以计算出下一次的r_{i+1}。推导过程如下：

由于是 Fp 上的椭圆曲线所以存在a^{-1}，满足：

$$a * a^{-1} = 1 \bmod p$$

然后有：

$$s_{i+1} = \varphi(x(s_i * P) = \varphi(x(s_i * a^{-1} * Q) = \varphi(x(a^{-1} * G)$$

其中的点 G 满足：

$$G = s_i Q$$
$$r_i = \varphi(x(G))$$

在已知r_i（G 的 x 坐标）情况下，可以根据椭圆曲线公式算出 G 的 y 坐标进而得到点 G，所以可求得s_{i+1}，即 DRBG 的内部状态。因此有：

$$r_{i+1} = \varphi(x(s_{i+1} * Q)$$

以此类推，攻击者可以得到后续所有的$r_j, (j \geq i)$，从而破坏了“不可预测”的性质。

事件联想

- 我们生活在一个不安全的环境
- Rand() 、random()
- Des、RSA、AES等等其他
- Microsoft CryptoAPI
- OpenSSL
- Inter芯片(黑色指令)

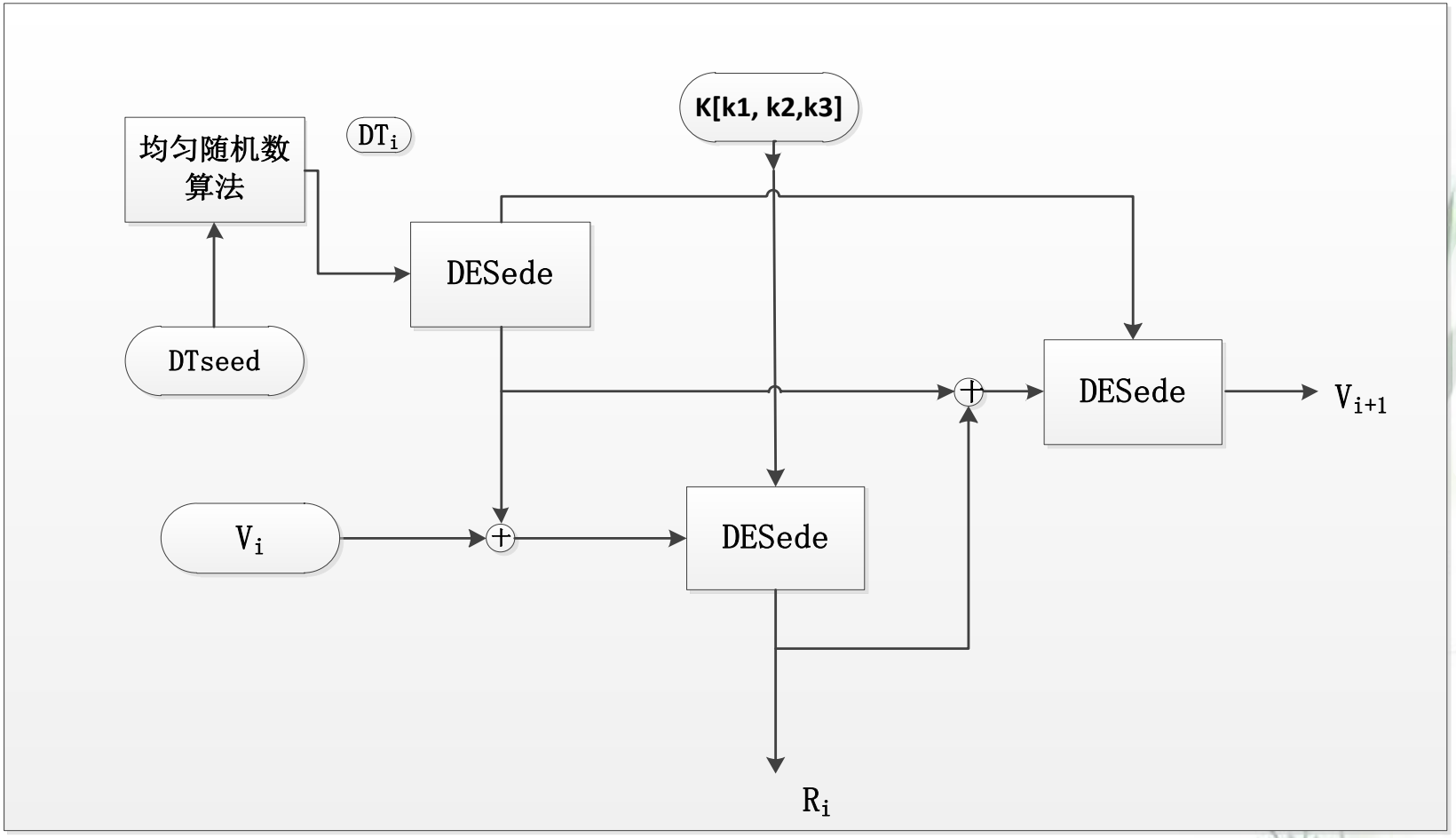
随机数生成器

- 应对措施：
  - 将Q换成随机生成的值
  - 自主研发

- 关于随机数生成器的研究国内国外很多
  - 基于硬件的真随机数生成器
  - 伪随机数生成器
    - 基于神经网络
    - 基于混沌理论
    - 超素数
    - 基于模糊控制
    - 对已有标准的改进

随机数生成器

- 一种改进的随机数生成器（ANSI X9.17）



谢谢观看！