软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2021,32(9):2887−2900 [doi: 10.13328/j.cnki.jos.005976]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel: +86-10-62562563

抗随机数后门攻击的密码算法*

康步荣[1,2,3], 张 磊[1,2,3], 张 蕊[1,2], 孟欣宇[1,2], 陈 桐[1,2]

[1](软硬件协同设计技术与应用教育部工程研究中心(华东师范大学),上海 200062)

[2](华东师范大学 软件工程学院,上海 200062)

[3](密码科学技术国家重点实验室,北京 100878)

通讯作者: 张磊, E-mail: leizhang@sei.ecnu.edu.cn

摘 要: 迄今为止,大多数密码原语的安全性都依赖于高质量的不可预测的随机数.密码学中,通常用伪随机数生成器(pseudorandom number generator,简称 PRNG)生成随机数.因此,密码算法中所用的 PRNG 的安全性将直接影响着密码算法的安全性.然而,近年来,越来越多的研究结果表明:在实际应用中,很多人为因素会导致 PRNG 生成的随机数是不随机或可预测的,称这种不安全的 PRNG 为有后门的 PRNG(backdoored pseudorandom number generator,简称 BPRNG).BPRNG 最典型的例子是双椭圆曲线伪随机数生成器(dual elliptic curves pseudorandom number generator,简称 Dual EC PRNG),其算法于 2014 年被曝出存在后门.BPRNG 的出现,使密码算法的研究面临着新的挑战.因此,研究抗随机数后门攻击的密码算法显得尤为重要.首先概述了抗随机数后门攻击密码算法的研究背景,然后着重对已有抗随机数后门攻击密码算法进行了总结和梳理.

关键词: 伪随机数生成器;随机数后门;抗随机数后门攻击;密码算法

中图法分类号: TP309

中文引用格式: 康步荣,张磊,张蕊,孟欣宇,陈桐.抗随机数后门攻击的密码算法.软件学报,2021,32(9):2887−2900. http://www.jos.org.cn/1000-9825/5976.htm

英文引用格式: Kang BR, Zhang L, Zhang R, Meng XY, Chen T. Cryptographic algorithms against backdoored pseudorandom number generator. Ruan Jian Xue Bao/Journal of Software, 2021,32(9):2887−2900 (in Chinese). http://www.jos.org.cn/1000-9825/5976.htm

Cryptographic Algorithms Against Backdoored Pseudorandom Number Generator

KANG Bu-Rong[1,2,3], ZHANG Lei[1,2,3], ZHANG Rui[1,2], MENG Xin-Yu[1,2], CHEN Tong[1,2]

[1] (Engineering Research Center of Software/Hardware Co-design Technology and Application, Ministry of Education (East China Normal University), Shanghai 200062, China)

[2](Software Engineering Institute, East China Normal University, Shanghai 200062, China)

[3](State Key Laboratory of Cryptology, Beijing 100878, China)

Abstract: So far, the security of the most of the cryptographic primitives depends on the high-quality and unpredictable randomness. In cryptography, the pseudorandom number generator (PRNG) is used to generate randomness. Thus, the security of the PRNG will directly impact the security of cryptographic algorithms. However, there have been some reports showing that many human factors can lead to the failure randomness generated by the PRNG which is referred to as the backdoored pseudorandom number generator (BPRNG). A good example of this BPRNG is the dual elliptic curves PRNG (Dual EC PRNG) which has been exposed to generate bad randomness. With the

* 基金项目: 国家重点研发计划(2017YFB0802000); 国家自然科学基金(61972159, 61572198); 软硬件协同设计技术与应用教育部工程研究中心主任基金(华东师范大学)

Foundation item: National Natural Science Foundation of China (2017YFB0802000); National Natural Science Foundation of China (61972159, 61572198); Dean's Fund of Engineering Research Center of Software/Hardware Co-design Technology and Application, Ministry of Education (East China Normal University)

收稿时间: 2019-07-11; 修改时间: 2019-09-28; 采用时间: 2019-11-04

emerging of BPRNG, new challenges will be confronted with the study of cryptographic algorithms. Therefore, it is important to investigate the cryptographic primitives against the BPRNG. This study first reviews the research background of the cryptographic primitives against the BPRNG, and then summarizes the existing schemes in this field.

Key words: PRNG; BPRNG; BPRNG resistance; cryptographic algorithms

迄今为止,大多数密码原语的安全性都依赖于高质量的不可预测的随机数[1−4].密码学中,我们通常用伪随机数生成器(pseudorandom number generator,简称 PRNG)来生成随机数.而实际上,很多人为因素会导致 PRNG 生成的随机数不安全[1−3,5].通常,我们称不安全的 PRNG 为存在后门的 PRNG(backdoored pseudorandom number generator,简称 BPRNG).在信息安全领域,后门是指可以绕过安全控制而获取对程序或系统访问权的方法.后门的最主要目的就是方便以后再次秘密进入或者控制系统.此处,我们所研究的后门主要是指存在于密码组件 PRNG 里的后门,这种后门使得 PRNG 产生的用于密码算法中的随机数,对于那些已知此后门的人来说是可预测的.知道后门的攻击者因可预测随机数,他很可能会成功破解相应的密码算法,这将严重地威胁到密码算法的安全性.正如在 2014 年 SXSW 大会(South By Southwest Conference)上斯诺登所言,攻击者在攻击加密算法时,真正受到攻击的其实是加密算法中使用的 PRNG,而非算法本身.所以,研究抵抗随机数后门攻击的密码算法是非常有意义且有必要的.

说起对密码算法的威胁,量子计算机也是其中之一.近年来,量子信息科学的研究和发展催生了量子计算机[6],而量子计算机的强大计算能力对传统密码算法,尤其是对公钥密码算法产生了严重威胁[6].例如,Shor 算法就是一个分解大整数问题和求解离散对数问题的有效量子算法[6,7].Shor 算法的出现,严重威胁了基于大整数分解困难问题和离散对数困难问题的公钥密码算法,如 RSA,ECC,ElGamal 算法等.文献[6]总结了现有的量子算法及其对传统公钥密码算法的威胁,并梳理了量子计算机在物理实现上的发展历史及相应成果.到目前为止,虽然国际上很多著名的公司都纷纷加入量子计算机的研制之中,但距离通用的量子计算机的大规模使用还需要很长时间.因此,在量子计算机真正取代传统计算机之前,随机数后门攻击成为威胁现有密码算法的主要因素.研究抗随机数后门攻击的密码算法是亟待解决的问题.

据统计,目前主要有两类影响 PRNG 工作过程的因素[1,2,5,8−10].

- 第 1 类影响因素是“漏洞”.例如,2006 年 9 月~2008 年 5 月发生在 Debian Linux 操作系统上的安全漏洞,一名程序员删除了 OpenSSL 密码库里的部分代码,导致该系统中 PRNG 的种子密钥仅剩 15 位熵[11].信息论中,熵用来表示一个数的不确定性,熵越大,数的不确定性越高.随后,传输层协议(transport layer security,简称 TLS)和安全套接字层协议(secure sockets layer,简称 SSL)被曝出其服务器的重要组件使用了有后门的 PRNG 而使协议存在安全漏洞[12];
- 第 2 类影响因素被称为“恶意颠覆”,其目的是减弱 PRNG 生成随机数的随机性.一个典型的例子是双椭圆曲线伪随机数生成器 Dual EC PRNG,Dual EC PRNG 是 NSA 设计的一个伪随机数生成器算法,由 NIST 列入算法标准[1,2,5,8−10,13,14].此后,Dual EC PRNG 一直被广泛使用,直至 2014 年,该算法被曝出存在后门,即生成的随机数可预测[15].在实际应用中,Dual EC PRNG 被著名网络公司 Juniper Network 应用于其所生产的 NetScreen VPN 路由器的操作系统中.在文献[16]中,作者详细分析了 NetScreen VPN 路由器所存在的该随机数后门攻击.

Dual EC PRNG 由两个算法组成[5]——密钥生成算法 $\boldsymbol{K}$ 和随机数生成算法 $\boldsymbol{G}$,可将其记为二元组 $PRNG=(\boldsymbol{K},\boldsymbol{G})$.Dual EC PRNG 是基于定义在有限域 F_p 上的椭圆曲线 $y^2=x^3+ax+b$ 设计的,这里,p 是一个素数.椭圆曲线上的所有点组成群 G,其生成元为 g,阶为 q.密钥生成算法 $\boldsymbol{K}$ 随机选取群元素 $Q\in G$ 和一个指数 $d\in Z_q$,计算 $P=Q^d$,输出公私钥对(pk,sk),其中,$pk=(P,Q)$对外公开,$sk=d$ 保密.S 表示一个状态空间,$S=Z_q$.随机数生成算法 $\boldsymbol{G}$ 输入 $s_i\in S$ 和公钥 pk,计算 $s_{i+1}=P^{s_i}$ 作为下一个状态值,计算 $r'_{i+1}=Q^{s_{i+1}}$,将 r'_{i+1} 的最后 16 位值去掉,用剩余位的值作为随机数 r_{i+1},算法 $\boldsymbol{G}$ 的输出为(s_{i+1},r_{i+1}).需要注意的是:这里,椭圆曲线上点的运算都是对其横坐标进行运算.Dual EC PRNG 的后门攻击是指一个攻击者如果已知私钥 d 和连续的两个随机数 r_1,r_2 的值,将 r_1,r_2 所对应的状态值记为 s,s_1,那么他可以有效地恢复出 s_2 的值.具体地,攻击者可以先对 r_1 进行后 16 位添加,恢复出 r'_1,共有 2^{16} 种可能性,

将每一种可能性记做 $X_i,i\in\{1,\ldots,2^{16}\}$.然后,攻击者计算检验 $Q^{x_i^d}$ 去掉最后 16 位的值后剩余位的值是否等于 r_2 的值:如果相等,他可以继续计算 $P^{s_1}=Q^{s_1^d}=X_i^d=s_2$,从而成功恢复出状态值 s_2.一旦攻击者恢复出正确的状态值 s_2,他就可以推算出所有后续的状态值和随机数.此次随机数后门攻击最多需要做 2^{16} 次运算,这对一个攻击者来说不难做到.

随着 Dual EC PRNG 后门事件的曝光,如何构造抵抗随机数后门攻击的密码算法,已逐渐成为密码学界广泛关注的一个重要话题.近几年,对于抗随机数后门攻击的密码算法的研究已经取得了一些有意义的结果,出现了各种抗随机数后门攻击的对称和公钥密码算法.本文就其中的主要结果进行了总结整理,从抗随机数后门攻击的对称加密算法、对冲公钥加密(hedged public-key encryption,简称 H-PKE)、基于随机性强化的方法、算法替代攻击等几个研究方向分析了目前抗随机数后门攻击密码算法的研究现状.通过分析已有相关构造的特点,我们指出,现有密码算法大多采用静态密码组件(如密钥生成器、PRNG 等).由于密码组件固化,这增加了算法设计者在设计算法时有意隐藏后门的可能性.鉴于这一发现,本文探讨将交叉动态思想引入密码算法设计之中,实现密码组件的动态组合优化;构造新型抗后门攻击密码算法,以达到抵抗后门攻击的目的.下面,我们对这些方法逐一进行概括与分析.

本文第 1 节介绍随机数后门攻击对密码算法的安全威胁和几种造成随机数后门攻击的原因.第 2 节~第 5 节分别从抗随机数后门攻击的对称加密算法、对冲公钥加密算法、基于随机性强化的方法以及其他相关技术等方面归纳相关研究方法的主要思想,并对各方法中需要进一步研究的问题进行分析.第 6 节对全文进行总结与展望.

1 抗随机数后门攻击的对称加密算法

对于加密算法,我们通常要求其能达到 CPA(chosen plaintext attacks)安全性.然而,经典的对称加密算法(如 AES,DES)未考虑该安全性.究其原因,这些算法为确定性加密算法.要实现 CPA 安全性,加密算法必须为概率性算法,即算法中需引入随机数(如加密模式中使用的初始化向量 IV、消息填充等).然而,若在算法实现时使用存在后门的 PRNG,则该加密算法将仍然无法达到 CPA 安全.本节介绍抗随机数后门的对称加密算法.

1.1 Kamara-Katz系列对称加密算法

Kamara-Katz 系列对称加密算法在 2008 年由 Kamara 和 Katz 提出[17],他们定义了两种新的对称加密算法的安全性质:CRA(chosen-randomness attacks,简称 CRA)安全性和 CCRA(control chosen-randomness attacks,简称 CCRA)安全性.CRA 安全性是指:即使敌手能询问加密预言机并完全控制算法中使用的随机数生成器,敌手也不能在多项式时间内恢复出给定密文所对应明文的任意部分信息.同时,作者还分析了 CRA 安全性和 CPA 安全性的关系[17].由于 CRA 安全性允许敌手完全控制算法的随机数生成器,所以严格意义上,CRA 安全性比 CPA 安全性更强.CCRA 安全性是指:即使敌手能询问加密预言机、解密预言机并完全控制算法中使用的随机数生成器,敌手也不能在多项式时间内恢复出给定密文所对应明文的任意部分信息.同样,他们将 CCRA 安全性和 CCA (chosen ciphertext attack,简称 CCA)安全性进行了对比[17].由于 CCRA 安全性允许敌手完全控制随机数生成器,所以本质上,CCRA 安全性比 CCA 安全性更强.Kamara-Katz 系列对称加密算法(symmetric key encryption,简称 SKE)包括 *SKE*1 与 *SKE*2[17].

*SKE*1 为抗随机数后门攻击的固定长度输出的对称加密算法,所谓固定长度是指被加密的明文消息及所对应密文的长度为固定值.该算法基于伪随机置换和伪随机函数构造.下面介绍 *SKE*1=(*Gen*,*Enc*,*Dec*)的具体算法.

- 密钥生成算法 $Gen(1^k)$:输入安全参数 k,该算法选取 $K_1,K_2\leftarrow\{0,1\}^k$,输出对称密钥 $K=\langle K_1,K_2\rangle$;
- 加密算法 $Enc_K(m,r)$:输入要加密的消息 m、随机数 $r\leftarrow\{0,1\}^k$ 和对称密钥 $K=\langle K_1,K_2\rangle$,计算 $c_2=F_{K_2}(r)\oplus m$,输出密文 $C=\langle c_1=P_{K_1}(r),c_2\rangle$.其中,$F$ 表示伪随机函数,P 表示伪随机置换,F 和 P 的输入输出都为 k 比特的固定长度;
- 解密算法 $Dec_K(c_1,c_2)$:输入密文 $C=\langle c_1,c_2\rangle$ 和对称密钥 $K=\langle K_1,K_2\rangle$,该算法计算 $r=P_{K_1}^{-1}(c_1)$,输出消息

$m = F_{K_2}(r) \oplus c_2$.

证明结果表明:在 P 是伪随机置换并且 F 是伪随机函数的假设成立时,上述方案满足 CRA 安全性.

*SKE*2 为抗随机数后门攻击的可变长度对称加密算法.*SKE*2 可以看作是 *SKE*1 的扩展算法,把消息空间扩展到无限长度.具体的 *SKE*2=(*Gen*,*Enc*,*Dec*)算法介绍如下.

- 密钥生成算法 $Gen(1^k)$:输入安全参数 k,该算法选取 $K_1,K_2 \leftarrow \{0,1\}^k$,输出对称密钥 $K=\langle K_1,K_2\rangle$;
- 加密算法 $Enc_K(m,r)$:将要加密的消息 m 分为 l 个长度为 k 的分量,即 $m=\langle m_1,\ldots,m_l\rangle$.该加密算法输入 $m=\langle m_1,\ldots,m_l\rangle$、随机数 $r \leftarrow \{0,1\}^k$ 和对称密钥 $K=\langle K_1,K_2\rangle$.对于 $1 \leqslant i \leqslant l$,计算 $c_i = F_{K_2}(r+i) \oplus m_i$,输出密文 $C = \langle P_{K_1}(r), c_1, ..., c_l\rangle$.其中,$F$ 表示伪随机函数,P 表示伪随机置换;
- 解密算法 $Dec_K(c_1,c_2)$:输入密文 $C=\langle c_1,c_2\rangle$和对称密钥 $K=\langle K_1,K_2\rangle$,该算法计算 $r = P_{K_1}^{-1}(c_0)$.对于 $1 \leqslant i \leqslant l$,计算 $m_i = F_{K_2}(r+i) \oplus c_i$,输出消息 $m=\langle m_1,\ldots,m_l\rangle$.

证明结果表明:在 P 是伪随机置换并且 F 是伪随机函数的假设成立时,算法 *SKE*2 满足 CRA 安全性.

1.2 需要进一步研究的问题

到目前为止,关于抗随机数后门攻击的对称加密算法的研究成果并不多,较为有效的算法仅有 Kamara-Katz 系列对称加密算法 *SKE*1,*SKE*2.但是我们不难发现,该算法的构造依赖于很强的假设条件.因为在算法实现过程中,很难保证所用的 P 函数和 F 函数是真正伪随机的,所以除了伪随机函数和伪随机置换之外,还可以用哪些数学工具和密码原语来构造抗后门攻击的对称密码算法,是一个需要研究的问题.另外,Kamara-Katz 系列对称加密算法相当于重新构造了一个对称加密算法,而不是在现有对称加密算法基础上构造.如何构造实用的抗随机数后门攻击的对称加密算法,即简单改变现有密码库(如 OpenSSL 库)的使用方式即可实现抗后门攻击,也是此研究领域的另一重要的有待解决的问题.这将大大减少密码库开发者的工作量,节省开发成本.

2 对冲公钥加密算法 H-PKE

对冲公钥加密算法最早由 Bellare 等人在 2009 年亚密会(ASIACRYPT)上提出[18].所谓对冲是指密码算法满足两个层次的安全性.

- 第 1 层安全性是指在加密算法中所用随机数是可靠的、高熵的情况下,算法可达到标准安全性(如 IND-CPA,IND-CCA);
- 第 2 层安全性是指在加密算法中所用随机数是不可靠的、低熵的情况下,算法依然可以满足某些比标准安全性稍弱的安全性,而不是直接被攻破[2,3,18].

当对冲公开密钥加密算法同时满足上述两个层次的安全性时,才说它是对冲安全的.对冲加密算法要求被加密的消息和加密时所用随机数的联合分布具有高熵.现有的对冲加密算法可以概括为 3 类,即确定性公钥加密(deterministic public-key encryption,简称 D-PKE)[2,18−20]、随机再确定性公钥加密算法(randomized-then-deterministic,简称 RtD)[2,18]、填充再确定性公钥加密(pad-then- deterministic,简称 PtD)[2,18].本节讨论对冲公钥加密的含义和安全性概念,然后分别从上述 3 个方面对现有方案进行总结和分析.

2.1 D-PKE算法

确定性公钥加密算法最早是由 Bellare 等人在 2007 年美密会(CRYPTO)上提出来的密码学原语[19].在文献[18]中,作者指出,确定性加密算法是构造对冲加密算法的一种方法.所谓确定性加密,本质上是指在算法设计中不使用随机数.他们指出,设计确定性公钥加密算法存在两个问题.

- 首先,如果一个敌手得知该算法的明文消息是从一个小的明文空间中选取的,那么他可以很容易用穷举法恢复出明文.为解决这个问题,他们要求算法的明文空间足够大,并且具有高的最小熵;
- 其次,因为在确定性公钥加密算中不使用随机数,所以加密算法输出的密文在某种程度上暴露了明文的部分信息.该问题的解决办法是要求明文不依赖于公钥,即明文和公钥是相互独立的.

文献[19]中提出了两个在随机预言模型下的确定性公钥加密算法实例:EwH 算法(encrypt-with-Hash,简称

EwH)和RSA-DOAEP算法(RSA-deterministic optimal asymmetric encryption padding,简称RSA-DOAEP).下面我们将对EwH算法和RSA-DOAEP算法分别进行讨论.简单来说,EwH算法是先对用户的公钥、明文消息做一次Hash操作,将Hash值作为一个安全公钥加密算法的随机数,并利用该公钥加密算法生成最终密文.下面我们给出具体的EwH加密算法.为方便描述,我们将EwH算法记为$EwH=(EwH.K,EwH.E,EwH.D)$,将任一安全公钥密码算法记为$PKE=(PKE.K,PKE.E,PKE.D)$,哈希函数记为$H:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^*$.

- 密钥生成算法$EwH.K(1^k)$:输入安全参数k,该算法运行算法$PKE.K(1^k)\to(pk,sk)$,输出公私钥对(pk,sk);
- 加密算法$EwH.E(pk,x)$:输入公钥pk和要加密的消息x,先计算$H(pk,x)\to R$,再运行算法$PKE.E(pk,x,R)\to y$,输出密文y;
- 解密算法$EwH.D(y,pk,sk)$:输入私钥sk、公钥pk和密文y,先计算$PKE.D(sk,y)\to x,H(pk,x)\to R$,再判断等式$PKE.E(pk,x,R)=y$是否成立:若成立,输出$x$;否则,输出$\perp$.

在文献[19]中,Bellare等人也同时分析了确定性公钥加密算法的安全性,给出了PRIV(privacy,简称PRIV)安全性的定义.PRIV安全性要求一个攻击者,已知一个明文向量所对应的确定性加密算法的密文,只要这个明文向量的每个分量有高的最小熵,则该攻击者不能在多项式时间内以不可忽略的概率猜出任何关于原明文的部分信息(部分信息不依赖于加密时所用的公钥).证明结果表明:如果公钥加密算法$PKE=(PKE.K,PKE.E,PKE.D)$是IND-CPA安全的,则上述EwH确定性加密算法满足PRIV安全性.

RSA-DOAEP算法是在RSA-OAEP算法对应的确定性算法,该算法先对明文消息进行填充,之后做3次Feistel计算,最后做一次RSA算法来生成相应的密文.RSA-DOAEP加密算法由3个基本算法组成,为方便描述,我们将其记为$RSA\text{-}DOAEP=(RSA\text{-}DOAEP.K,RSA\text{-}DOAEP.E,RSA\text{-}DOAEP.D)$.该算法有两个基础参数:$k_0,k_1>0$,他们之间满足关系$n>2k_0$和$n\geqslant k_1$.这里,$n$表示明文长度.算法的明文空间为$\max(k_1,2k_0+1)$,RSA算法的模数为$N=k_1$.$H_1,H_2:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^{k_0}$,$R:\{0,1\}^*\times\{0,1\}^*\to\{0,1\}^{n-k_0}$表示哈希函数.算法描述中,我们用$s[i\ldots j]$表示字符串$s$的第$i$到第$j$个比特.RSA-DOAEP算法的具体描述如下.

- 密钥生成算法$RSA\text{-}DOAEP.K(1^k)$:输入安全参数k,算法输出RSA算法的公私钥对$pk=(N,e),sk=(N,d)$;
- 加密算法$RSA\text{-}DOAEP.E((N,e),x)$:输入明文消息$x$和公钥$pk=(N,e)$,计算$x_l\leftarrow x[1\ldots k_0],x_r\leftarrow x[k_0+1\ldots n]$,$s_0\leftarrow H_1((N,e),x_r)\oplus x_l,t_0\leftarrow R((N,e),s_0)\oplus x_r,s_1\leftarrow H_2((N,e),t_0)\oplus s_0,x_1\leftarrow(s_1\|t_0)[1\ldots n-k_1],x_2\leftarrow(s_1\|t_0)[n-k_1+1\ldots n]$,$y\leftarrow x_1\|(x_2^e \bmod N)$,输出密文$y$;
- 解密算法$RSA\text{-}DOAEP.D((N,d),y)$:计算$x_1\leftarrow y[1\ldots n-k_1],y_1\leftarrow y[n-k_1+1\ldots n]$,$x\leftarrow x_1\|(y_1^e \bmod N)$,$s_1\leftarrow x[1\ldots k_0],t_0\leftarrow x[k_0+1\ldots n],s_0\leftarrow H_2((N,e),t_0)\oplus s_1,x_r\leftarrow R((N,e),s_0)\oplus t_0,x_l\leftarrow H_1((N,e),x_r)\oplus s_0$,输出明文$x_l\|x_r$.

证明结果表明,上述确定性加密算法RSA-DOAEP是PRIV安全性.

关于确定性加密算法的研究还有一些其他的研究结果,例如在文献[20]中,Boldyreva等人在文献[19]的基础上继续研究了确定性公钥加密算法的设计及安全性定义,他们发现了确定性公钥加密和有损限门函数之间的联系.他们利用有损限门函数,给出了在标准模型下满足PRIV-CPA安全性(即,在PRIV安全性的基础上允许攻击者进行加密预言机询问)的确定性公钥加密算法的一般性构造思想.为了更好地描述该算法,他们提出了一个新的密码原语,隐藏全域哈希模式的确定性公钥加密算法(deterministic encryption with hidden universal-Hash mode,简称DEHUHM);其次,他们将该PRIV-CPA安全的算法构造进行了扩展,给出了PRIV-CCA安全的确定性加密算法的一般性构造.另外,文献中还基于抗目标碰撞哈希函数、DDH困难问题给出了两个具体的确定性加密算法实例.

2.2 RtD算法

Bellare等人在文献[18]中介绍了对冲公钥密码算法RtD,RtD基本思想是:对消息m先用一个概率性加密算法进行加密,输出密文C',再用一个确定性加密算法对C'进行加密,输出最终密文C.同时,他们定义了一个新的对冲公钥加密算法的安全性质,即选择分布攻击下的不可区分性(indistinguishability under chosen-distribution attacks,简称IND-CDA).在被加密的明文消息和相应随机数的联合分布是高熵的条件下,一个对冲公钥加密算

法才能满足 IND-CDA 安全性.Bellare 等人表示:IND-CDA 安全性本质上是对 PRIV 安全性的一种变形,两者的关系是适应性 IND-CDA 安全性比 PRIV 安全性强,而非适应性 IND-CDA 安全性等价于 PRIV 安全性.下面给出具体的 RtD=($RtD.P$,$RtD.K$,$RtD.E$,$RtD.D$)构造.为方便起见,我们将随机性公钥密码算法记为 $RPKE$=($RPKE.P$, $RPKE.K$,$RPKE.E$,$RPKE.D$),将确定性公钥密码算法记为 $DPKE$=($DPKE.P$,$DPKE.K$,$DPKE.E$,$DPKE.D$).

- 参数生成算法 $RtD.P(1^k)$:输入安全参数 k,先运行算法 $RPKE.P(1^k)\rightarrow Par_r$,得到随机性公钥密码算法 RPKE 的系统参数 Par_r;再运行算法 $DPKE.P(1^k)\rightarrow Par_d$,得到确定性公钥密码算法 DPKE 的系统参数 Par_d,输出(Par_r,Par_d);
- 密钥生成算法 $RtD.K(1^k)$:输入安全参数 k,运行算法 $RPKE.K(Par_r)\rightarrow(pk_r,sk_r)$和 $DPKE.K(Par_d)\rightarrow(pk_d, sk_d)$,输入算法的公私钥对($pk$=($pk_r$,$pk_d$),$sk$=($sk_r$,$sk_d$));
- 加密算法 $RtD.E((pk_r,pk_d),m,r)$:输入公钥 pk=(pk_r,pk_d)、被加密消息 m 和一个随机数 r,先计算 $RPKE.E(pk_r,m,r)\rightarrow c$,再计算 $DPKE.E(pk_d,c||10^l)\rightarrow C$,输出密文 C.其中,$l=n_d-|c|-1$,n_d 表示 DPKE 算法的明文长度,0^l 表示有 l 个 0;
- 解密算法 $RtD.D(C,(sk_r,sk_d))$:输入私钥 sk=(sk_r,sk_d)和密文 C,计算 $DPKE.D(sk_d,C)\rightarrow c$,$RPKE.D(sk_r,c)\rightarrow m$, 输出 m.

证明结果表明:若公钥加密算法 $RPKE$=($RPKE.P$,$RPKE.K$,$RPKE.E$,$RPKE.D$)是 IND-CPA 安全的,则上述 RtD 构造满足 IND-CDA 安全性.

2.3 PtD算法

PtD 也是 Bellare 等人在文献[18]中提出的一种构造对冲公钥加密算法的方法.所谓的 PtD 加密是指先对消息 m 进行填充,输出 m',再用一个确定性加密算法对 m'进行加密,输出最终的密文 C.下面介绍具体的 PtD=($PtD.P$,$PtD.K$,$PtD.E$,$PtD.D$)加密算法,我们将确定性公钥密码算法记为:$DPKE$=($DPKE.P$,$DPKE.K$,$DPKE.E$, $DPKE.D$).

- 参数生成算法 $PtD.P(1^k)$:输入安全参数 k,运行确定性加密算法的参数生成算法 $DPKE.P(1^k)\rightarrow Par_d$,输出确定性公钥加密算法的系统参数 Par_d;
- 密钥生成算法 $PtD.K(Par_d)$:输入系统参数 Par_d,运行确定性公钥加密算法的密钥生成算法 $DPKE.K(Par_d)\rightarrow(pk_d,sk_d)$,输出公私钥对($pk_d$,$sk_d$);
- 加密算法 $PtD.E(pk_d,m,r)$:输入系统参数 Par_d、随机数 r、明文 m,运行确定性公钥加密算法 $DPKE.E(pk_d,r||m)\rightarrow C$,输出密文 C;
- 解密算法 $PtD.D(C,sk_d)$:输入密文 C,私钥 sk_d,运行解密算法 $DPKE.D(sk_d,C)\rightarrow m$,输出消息 m.

证明结果表明,上述对冲加密算法 PtD=($PtD.P$,$PtD.K$,$PtD.E$,$PtD.D$)满足 IND-CDA 安全性.

在 2017 年的美密会上,Boldyreva 等人从实际出发,研究了在密码库 OpenSSL 中可实现的对冲加密算法以及对冲加密算法的安全性质[2].他们定义了两个新的对冲安全性质,即 MM-CCA(message-message security against chosen ciphertext attack)和 MMR-CCA(message-message-randomness security against chosen ciphertext attack).作者指出,第 2.2 节、第 2.3 节中所述的 IND-CDA 安全性等价于 MMR-CPA 安全性(message-message-randomness security against chosen plaintext attack).文献[18]的研究结果已经表明:RtD 算法和 PtD 算法在满足一定约束条件时可达到 IND-CDA 安全性,即 MMR-CPA 安全性.所以在文献[2]中,Boldyreva 等人将该结果进行扩展,研究了 RtD 算法和 PtD 算法相应的 CCA 安全性.证明结果表明,对于 RtD 算法,当确定性算法选用 RSA-DOAEP 时,算法可达到 MM-CPA 和 IND-CPA 安全;当概率性算法选用关联数据的单射加密算法,则算法可达到 MMR-CCA 和 IND-CCA 安全性.而对于 PtD 算法,当确定性算法选用 RSA-DOAEP 时,算法可满足 MM-CCA 和 IND-CCA 安全性.同时,文献[2]中的作者还基于关联数据的可验证加密算法和陷门置换函数构造了一个混合加密算法,并给出安全性分析.结果表明,该混合加密算法可满足 MMR-CCA 和 IND-CCA 安全性.他们的另一研究结果表示, RSA-OAEP 算法在随机预言模型中可达到 MM-CCA 安全性.这在实际应用中非常有意义,因为 RSA-OAEP 包含在现有很多密码库中,可直接访问现有密码库的中的高级程序接口而易于实现.

2.4 有待深入研究的问题

关于对冲公钥加密算法,我们总结了如下几个需要进一步研究的问题.

1) 现有对冲公钥加密算法都依赖随机预言模型,而该模型是密码学中的一个理想化模型,现实世界中并不存在.如何构造基于标准模型下的对冲公钥机密算法,将是值得继续研究的一个方向;
2) 目前,关于对冲公钥加密算法的安全性研究存在一个一般性问题,就是没有一个安全性质可以适用于所有的对冲公钥加密算法.所以,研究对冲公钥加密算法的一般性安全性质是值得探索的方向;
3) 对冲公钥加密算法通常要求明文消息和相应随机数(或随机填充值)的联合分布是高熵的.若明文空间较小,对冲公钥加密算法的安全性等价于随机数生成算法的安全性.因此,设计明文空间较小情况下,抗后门攻击的对冲公钥加密算法,是一个值得探索的方向.

3 基于随机性强化的方法

本节讨论基于随机性强化的抗随机数后门攻击方法.目前,基于随机性强化的方法可以概括为 3 类,即 nonce-based 公钥加密算法(nonce-based public-key encryption,简称 N-PKE)[1,4,21,22]、对冲的 nonce-based 公钥加密算法(hedged nonce-based public key encryption,简称 HN-PKE)[3]、Dodis 随机数生成算法[5].以下对这 3 种方法分别进行总结.

3.1 N-PKE算法

Nonce-based 公钥加密算法的发展可以追溯到 2002 年,Rogaway 在关联数据的可验证加密方案中首次引入了 nonce 的概念[21].2004 年,Rogaway 首次提出 nonce-based 对称加密方案[4].2006 年,Rogaway 和 Shrimpton 细化了 nonce 的概念[22].他们表示:packet sequence numbers 即可作为一个 nonce,并且强调 nonce-based 加密思想可以有效抵抗随机数后门攻击.2016 年,Bellare 和 Tackmann 提出了 nonce-based 公钥密码算法[1].

在文献[1]中,Bellare 和 Tackmann 定义了 nonce-based 公钥密码算法应满足的安全属性,并给出了具体构造和安全性分析.相比于传统公钥密码算法,nonce-based 公钥密码算法中需要使用两个额外的密码组件,即 nonce 生成器(nonce generator,简称 NG)和对冲提取器(hedged extractor,简称 HE).

- 前者的输入为安全参数 k、nonce selector η和当前状态值 St,输出为 nonce 值 n 和下一个状态值 St';
- 后者输入为安全参数 k,种子密钥 xk、消息 M 和 nonce n,输出一个随机数 r.

Bellare 和 Tackmann 分别给出了 HE 在随机预言模型和标准模型下的构造方法[1].

在随机预言模型下 HE 的构造,需把 HE 看作随机预言机 RO.假设 k 是种子密钥的长度,l 是 HE 的输出长度,$HE.Keys=\{0,1\}^k$,$HE.Dom=\{0,1\}^*\times\{0,1\}^*$,$HE.Rng=\{0,1\}^l$,其中,$HE.Dom$ 是(n,M)的取值空间.HE 可定义为映射 $HE:HE.Keys\times HE.Dom\rightarrow HE.Rng$.具体 HE 的构造为 $HE^{RO}(xk,(n,M))$,其中,xk 为种子密钥,$n\in\{0,1\}^*$为 nonce 值,$M\in\{0,1\}^*$表示消息.为保证构造的安全性,HE 需视作 RO,即 $HE^{RO}(xk,(n,M))=RO((xk,(n,M)),l)$.

标准模型下,HE 的构造基于伪随机函数 PRF(pseudorandom function)和 AXUHF(almost XOR universal Hash function).将 PRF 记为映射 $F:F.Keys\times(\{0,1\}^*\times\{0,1\}^*)\rightarrow\{0,1\}^l$,将 AXUHF 记为映射 $H:H.Keys\times H.Dom\rightarrow\{0,1\}^l$.其中,$F.Keys$ 和 $H.Keys$ 分别表示 PRF 和 AXUHF 的密钥空间,$H.Dom\subseteq\{0,1\}^*$表示 nonce 值的取值空间.假设种子密钥为 xk、nonce 值为 $n\in H.Dom$、消息为 $M\in\{0,1\}^*$,标准模型下 HE 的构造如下.

- 先将 xk 分为两部分,即 $xk\rightarrow(hk,fk)$,其中,hk 和 fk 分别属于 $H.Keys$ 和 $F.Keys$;
- 分别执行 PRF 和 AXUHF,即 $H(hk,n)\rightarrow z_1$,$F(fk,(M,n))\rightarrow z_2$;
- 最终,HE 的输出为 $z_1\oplus z_2\in\{0,1\}^l$.

Nonce-based 公钥加密算法基于一个传统安全的公钥加密算法设计[1].下面介绍具体的 nonce-based 公钥加密算法.为方便起见,我们将其记做 $NPKE=(NKg,NSKg,NEnc,NDec)$,将所用的传统安全的公钥加密算法记为 $PE=(PE.Kg,PE.Enc,PE.Dec)$.一个 nonce-based 公钥加密算法包括如下 4 个基本算法.

- 密钥生成算法 $NKg(1^k)$:输入安全参数 1^k,运行算法$(pk,sk)\leftarrow PE.Kg(1^k)$,输出公私钥对$(pk,sk)$;

- 种子密钥生成算法 $NSKg(1^k)$:输入安全参数 1^k,输出种子密钥 xk;
- 加密算法 $NEnc(pk,M,xk)$:输入公钥 pk、消息 M、种子密钥 xk,先运行 NG 算法生成 nonce 值 n,即 $(n,St')\leftarrow NG(\eta,St)$,其中,nonce selector η和 NG 的当前状态值 St 是加密者自己选取的,St'表示 NG 的下一个状态值;再运行 HE 算法生成随机数 r,即 $r\leftarrow HE^{RO}(xk,M,n)$;再运行算法 $PE.Enc$ 进行加密操作,即 $C\leftarrow PE.Enc(pk,M,r)$;最后输出密文 C;
- 解密算法 $NDec(sk,C)$:输入私钥 sk 和密文 C,运行算法 $M\leftarrow PE.Dec(sk,pk,C)$,输出消息 M.

对于 nonce-based 公钥加密算法,若一个攻击者想攻破该算法,他需要同时获得 nonce 和种子密钥的值[1].文献[1]中,Bellare 和 Tackmann 定义了两个 nonce-based 公钥加密算法的安全性质,即 NBP1(nonce-based privacy 1)和 NBP2(nonce-based privacy 2).

- NBP1 是指攻击者未知用户的种子密钥时,只要消息和 nonce 不重复,攻击者就不能攻破 nonce-based 公钥加密算法;
- NBP2 是指攻击者已知用户种子密钥时,只要 nonce 不可预测,攻击者就不能攻破密码算法.

Bellare 和 Tackmann 指出:对于上述 NPKE 算法,若其采用标准模型下的 HE 和标准模型下可证明安全的 PE 算法,则 NPKE 算法在标准模型下满足 NBP1 和 NBP2 安全性;否则,只要 NPKE 中采用了随机预言模型下的 HE 或 PE,则 NPKE 在随机预言模型下满足 NBP1 和 NBP2 安全性[1].

另外,Bellare 和 Tackmann 还研究了 nonce-based 签名方案,并对其安全性进行分析和证明[1].Nonce-based 签名方案的设计基于一个传统的数字签名算法.下面介绍具体的 nonce-based 签名算法,为方便起见,我们将其记做 $NDS=(NDS.Kg,NDS.Sig,NDS.Vrf)$,将所用的传统签名算法记为 $DS=(DS.Kg,DS.Sig,DS.Vrf)$.一个 nonce-based 公钥加密算法包括如下 3 个基本算法.

- 密钥生成算法 $NDS.Kg(1^k)$:输入安全参数 1^k,运行算法 $(sk,vk)\leftarrow DS.Kg(1^k)$,输出签名密钥 sk,验证密钥 vk 以及种子密钥 xk;
- 签名算法 $NDS.Sig(1^k)$:输入签名密钥 sk、种子密钥 xk、消息 M,先运行 NG 算法生成 nonce 值 n,即 $(n,St')\leftarrow NG(\eta,St)$,其中,nonce selector η和 NG 的当前状态值 St 是加密者自己选取的,St'表示 NG 的下一个状态值;再运行 HE 算法生成随机数 r,即 $r\leftarrow HE^{RO}(xk,M,n)$;再运行算法 $DS.Sig$ 进行签名操作,运行算法 $s\leftarrow DS.Sig(sk,M,r)$,输出签名 s;
- 验证算法 $NDS.Vrf(1^k)$:输入验证密钥 vk、消息 M 和签名 s,若等式 $NDS.Vrf(vk,M,NDS.Sig(sk,xk,M,n))=1$,则表示签名认证成功;否则,输出错误符号$\perp$.

文献[1]中定义了 nonce-based 签名算法的两个安全性质,即 NBUF1(nonce-based unforgeability 1)和 NBUF2 (nonce-based unforgeability 2).

- NBUF1 是指:只要种子密钥保密的情况下,不论 nonce 值是否可预测,则 nonce-based 签名算法都能满足不可伪造性;
- NBUF2 是指:种子密钥泄露的情况下,只有 nonce 值不可预测时,nonce-based 签名算法才能满足不可伪造性.

Bellare 和 Tackmann 指出:对于上述 NDS 算法,若其采用标准模型下的 HE 和标准模型下可证明安全的 DS 算法,则 NDS 算法在标准模型下满足 NBUF1 和 NBUF2 安全性;否则,只要 NDS 中采用了随机预言模型下的 HE 或 DS,则 NDS 在随机预言模型下满足 NBUF1 和 NBUF2 安全性[1].

3.2 HN-PKE算法

2018 年,Huang 等人在文献[3]中首次将对冲公钥加密和 nonce-based 公钥加密相结合,提出了对冲的 nonce-based 公钥加密算法.从本质上讲,对冲的 nonce-based 公钥加密着眼于研究 nonce-based 公钥加密算法(详见第 3.1 节)的对冲安全性质,即:当 nonce-based 公钥加密算法中所用的随机数存在后门时,算法不是直接被攻破,而是仍然可以满足某些弱的安全性.文献[3]中,作者将第 2.2 节介绍的对冲安全性质 IND-CDA 进行了扩展,在其基础上定义了一个新的适用于 nonce-based 公钥加密算法的安全性质 IND-CDA2(chosen-ciphertext security

against chosen-distribution attack);并且他们指出,IND-CDA2 安全性比 IND-CDA 安全性更强.IND-CDA2 安全性要求 nonce-based 公钥加密算法中对冲提取器 HE 的种子密钥、被加密明文消息以及随机数的联合分布有高的最小熵.对冲的 nonce-based 公钥加密算法需要同时满足 IND-CDA2,NBP1,NBP2 这 3 种安全性.除此之外,文献[3]中还分析证明了 IND-CDA2 与 NBP1/NBP2 之间的关系,他们的证明结论表示,NBP1/NBP2⇏IND-CDA2,IND-CDA2⇏NBP1/NBP2.Huang 等人表示,第 3.1 节介绍的 nonce-based 公钥加密算法即可视作在随机预言模型下 HN-PKE 的算法构造.他们着重研究了 nonce-based 公钥加密算法的对冲安全性质,证明结果表明,nonce-based 公钥加密算法在随机预言机模型下满足 IND-CDA2 安全性.

另外,Huang 等人考虑了 HN-PKE 在标准模型下的算法构造,并提出了一个具体的 NtD(nonce-then-deterministic)加密算法[3].所谓的 NtD 算法是指:先用 nonce-based 公钥加密算法 N-PKE(详见第 3.1 节)对明文消息 m 进行加密生成 m',再选择一个确定性加密算法 D-PKE 对 m'进行加密,生成最终密文 C.具体的 NtD 算法包含 4 个基本算法,分别是密钥生成算法 $NDKg$、种子生成算法 $NDSKg$、加密算法 $NDEnc$、解密算法 $NDDec$,我们将其记为 $NtD=(NDKg,NDSKg,NDEnc,NDDec)$.为方便起见,我们将 N-PKE 算法记为 $NPKE=(NKg,NSKg,NEnc,NDec)$,将 D-PKE 算法记为 $DPKE=(DKg,DEnc,DDec)$.具体的 NtD 加密算法介绍如下.

- 密钥生成算法 $NDKg(1^k)$:输入安全参数 1^k,首先运行 N-PKE 算法的密钥生成算法 $NKg(1^k)\rightarrow(pk_n,sk_n)$,生成 N-PKE 算法的公私钥对;其次运行 D-PKE 算法的密钥生成算法 $DKg(1^k)\rightarrow(pk_d,sk_d)$,生成 D-PKE 算法的公私钥对;最后输出 NtD 算法的公钥 $pk=(pk_n,pk_d)$,私钥 $sk=(sk_n,sk_d)$;
- 种子生成算法 $NDSKg(1^k)$:输入安全参数 1^k,运行 N-PKE 算法的种子生成算法 $NSKg(1^k)\rightarrow xk$,输出种子密钥 xk;
- 加密算法 $NDEnc_{pk}(M,n,xk)$:输入公钥 $pk=(pk_n,pk_d)$、消息 M、一个 nonce 值 n,先运行 N-PKE 算法的加密算法 $NEnc(pk_n,xk,M,n)\rightarrow y$,再运行 D-PKE 算法的加密算法 $DEnc(pk_d,y)\rightarrow C$,输出密文 C,其中,nonce 由 NG 产生;
- 解密算法 $NDDec_{sk}(C)$:输入私钥 $sk=(sk_n,sk_d)$和密文 C,先运行 D-PKE 算法的解密算法 $DDec(sk_d,C)\rightarrow y$,再运行 N-PKE 算法的解密算法 $NDec(sk_n,y)\rightarrow M$,输出消息 M.

证明结果表明:当确定性加密算法 $DPKE=(DKg,DEnc,DDec)$在标模下满足适应性 CCA 安全性时,NtD 算法在标模下满足 NBP1,NBP2,IND-CDA2 安全性.

3.3 Dodis随机数生成算法

在文献[5]中,Dodis 等人详细介绍了 Dual EC PRNG 中后门攻击的原理.同时,他们表示,可以用密钥封装算法和公钥加密算法来构造 BPRNG.即,将密钥封装算法和公钥加密算法的输出看作 BPRNG 生成的随机数.

除此之外,他们还提出了一种用于增强 PRNG 输出随机性的函数,将该函数定义为“免疫”函数,用 f_{seed} 表示.“免疫”函数的工作原理是:将可能存在后门的 PRNG 生成的可能不安全的可预测随机数做为“免疫”函数 f_{seed} 的输入,将函数 f_{seed} 的输出作为最终的随机数.

这种情况下,如何判断“免疫”函数作用的有效性是个重要问题.文献[5]中给出了一种验证方法:存在一个攻击者 A,他试图构造一个带有后门的 PRNG,然后使用“免疫”函数 f_{seed} 对该 PRNG 进行免疫.如果 A 能成功构造一个带有后门的 PRNG,并绕过 f_{seed},则表明函数 f_{seed} 为无效免疫;否则,表明 f_{seed} 有效免疫.在这个验证过程中,根据攻击者已知“免疫”函数 f_{seed} 相关信息的程度不同,Dodis 等人将免疫模型分为 3 种:公开免疫模型、半隐私免疫模型和隐私免疫模型.其中:公开免疫模型是指攻击者 A 构造带有后门的 PRNG 之前就已知函数 f_{seed} 的 $seed$ 值,也就是说,攻击者已知函数 f_{seed};半隐私免疫模型是指 A 构造带有后门的 PRNG 之后才已知 $seed$;隐私免疫模型是指 A 构造带有后门的 PRNG 前后都未知 $seed$.Dodis 等人的研究结果表明:在公开免疫模型下,存在后门的 PRNG 是不能被免疫的,即不存在免疫函数 f_{seed}.在半隐私免疫模型下,Dodis 等人分别考虑了针对随机预言模型和标准模型的免疫函数.他们指出:在随机预言模型下,可将随机预言机 RO(random oracle)看作免疫函数,即 $f_{seed}=RO$;在标准模型下,可用通用计算萃取器 UCE(universal computational extractor)作为免疫函数,即 $f_{seed}=UCE$;在隐私免疫模型下,Dodis 等人指出:可将伪随机函数 PRF 作为免疫函数,即 $f_{seed}=PRF$.

3.4 需要进一步研究的问题

基于随机性强化的抗随机数后门攻击方法本质上是一种门限机制,即随机数的生成依赖多个密码组件.当单个或若干个密码组件存在后门时,只要某个密码组件是安全可靠的,仍然可以得到安全的随机数.虽然门限机制可有效解决后门攻击问题,然而现有方案还存在如下问题.

1) 在 nonce-based 公钥加密算法中,一个新的密码组件 HE 被用于增强随机性.然而,根据文献[1]中所给 HE 的定义可以看出,HE 的实例化依赖于随机预言机 RO 或者依赖于 AXUHF 和 PRF.而 RO 是密码学中的一个假设,现实世界并不存在.此外,作者并没给出随机预言模型下,HE 的具体构造.因此在实际应用中,如何实现该类 HE 还需进一步研究.在标准模型下,HE 的实例化依赖于 AXUHF 和 PRF,而现有已实现的 AXUHF,PRF 等密码学工具中是否存在类似于 Dual EC PRNG 随机数后门攻击,也还有待研究;
2) 第 3.3 节所述的"免疫"函数的实现也存在上述类似的问题.现有"免疫"函数的实现依赖于 RO,UCE 或 PRF.RO 和 UCE 都在密码学中的一个假设,而已实现的 PRF 中是否存在随机数后门攻击等问题,还有待研究.此外,作者也未给出具体的免疫函数;
3) 在文献[3]中,作者考虑了对冲公钥加密算法在标准模型下的构造,并提出了 NtD 对冲公钥加密算法(详见第 3.3 节).该算法的安全性依赖于完全适应性 CCA 安全的确定性加密算法,然而如何构造适应性 CCA 安全的确定性加密算法,目前还是一个开放问题[3].

4 其他相关技术

上述抗随机数后门攻击密码算法侧重于算法层面的安全性.在实际应用中,攻击者可在算法实现时设计后门来破坏密码系统的安全性,其中最典型的为算法替代攻击.本节首先阐述算法替代攻击基本原理,随后介绍现有抵抗算法替代的方法.

4.1 算法替代攻击

算法替代攻击(algorithm substitution attacks,简称 ASA)最早由 Young 等人在 1997 年欧密会(EUROCRYPT)上提出[23],该攻击也称为颠覆攻击(substitution attacks,简称 SA).相较于在算法中设计后门,算法替代攻击着重于在密码算法实现过程中插入后门.通常来说,密码系统中使用的密码算法的安全性是经过严格的安全性分析的.然而在实际应用中,这些密码系统的使用模式是"黑盒"模式[24],即用户并不知晓其内部构造.这使得攻击者可恶意设计算法的使用模式,在特殊情况下,用新算法覆盖掉原有算法,同时,新算法即使面对相当密集的黑盒测试也会看起来完全安全.在文献[25]中,作者指出,所有依赖第三方软件库或硬件设备的密码系统均可能遭受算法替代攻击.

算法替代攻击的基本原理是:攻击者在密码算法从理论转化为现实过程中,将原诚实可靠的实现算法替换成一个已被植入秘密信息的替代算法[26].植入的秘密信息只有敌手可见,通常称为后门信息.攻击者可利用该后门信息与输出结果的联系来恢复系统的秘密信息(如密钥、随机数等),从而破坏系统的安全性.ASA 攻击要求对于除攻击者以外的任意用户来说,替代算法与诚实算法的输出分布结果是不可区分的.随着对算法替代攻击的不断研究,如何有效抵御算法替代攻击也成为一个新的问题.最简单的防算法替代攻击的策略是采用确定性密码算法[8],如文献[8,25–27]中所建议的加密方案、本文第 2.1 节中所介绍的确定性加密算法等.因确定性加密算法具有唯一密文属性,攻击者若在算法实现时插入后门,其攻击行为将很容易被检测到.然后,如第 2.1 节所述,为保证算法的安全性,确定性加密算法要求明文空间足够大,并且具有高的最小熵.

近年来,针对概率性密码算法的 ASA 防御策略的研究也取得了一定的进展,目前大致分为两类:第 1 类被称作为抗盗密密码学(cliptography)[28],详见第 4.2 节;第 2 类被称为逆向防火墙[29,30],详见第 4.3 节.

4.2 抗盗密密码学

抗盗密密码学的概念最初是由 Alexander 和 Tang 等人[25]提出的,旨在防止盗密攻击(kleptographic)下[20],

概率性密码算法免受算法替代攻击的威胁.抗盗密密码学借鉴了模块化的设计思想,即原密码算法可划分成不同的算法组件(子模块),每个算法组件可独立执行.此外,抗盗密密码学采用有威慑力的可信第三方实体——看门狗”(watchdog)来检测每个算法组件是否遭受算法替代攻击.抗盗密密码学的关键在于如何划分算法组件,文献[28]中的“split-program”模块化方法根据算法执行过程中是否需要使用随机数而将整个算法分成两个模块:确定性算法组件(例如确定性加密算法)和概率性算法组件(例如随机数生成算法、密钥生成算法).两个模块独立执行,具体的,先执行概率性算法组件,并将执行结果输入到一个散列函数中,再将经过该函数作用过的结果输入到确定性算法组件去执行.由于原算法被分为多个独立组件,因此攻击者需对所有组件一一替换.模块化设计的思想在于增加了攻击者替换原算法的难度,散列函数的作用则在于增加随机数的熵值和不确定性.此外,Alexander 等人在文献[28]基础上提出了“double-split”方法[31,32].该方法在“split-program”划分的基础上,将概率性算法组件分为两个子组件.子组件独立且并发执行,执行结果级联后输入散列函数.后续执行过程与文献[28]类似.

目前,抗盗密密码学只是初具雏形,有关的潜在应用场景还值得进一步研究,譬如利用该方法构造一个 collusion-free 的协议[33].此外,该方法主要考虑无状态算法[34].在一些实践中,算法可能是有状态的[28],例如计数器模式加密.如何扩展到有状态的算法,还值得深入研究.

4.3 逆向防火墙

传统防火墙用于内网和外网的隔离,它按照系统管理员预先定义好的规则来控制数据包的进出,以阻挡来自外网的入侵,保障内网的安全.密码逆向防火墙(cryptographic reverse firewalls,简称 CRF)的概念最初是由 Mironov 等人在 2015 年的欧密会上提出的[35].密码逆向防火墙旨在防止机密信息从内网遭受入侵(密码算法存在算法替代攻击)的主机中泄露出去,其基本思想在于重随机化[36,37−39].密码逆向防火墙的关键在于设计/找到合适的加密算法,该算法能确保公钥/密钥或是密文被重随机化后,接收方仍能正确解密.例如:在公钥密码体制中,发送者用公钥加密生成的密文从内网发出时,为防止加密算法被替换为植入后门信息的算法而破坏算法安全性,密文会被密码逆向防火墙重随机化后发给接收者,接收者可直接解密该密文.密码逆向防火墙也可基于公钥/密钥重随机化[40],该类方法旨在抵抗攻击者在公钥中植入后门信息.此时要求选择的加密算法具有密钥可延展性(key malleable),即,接收者可把使用重随机后的公钥加密的密文映射到用原始公钥加密的密文[41,42].找到拥有这样的可重随机化特性的加密算法并设计相应的密码逆向防火墙,是当下的主要研究内容.

目前为止,密码逆向防火墙仍有一些问题亟待解决,其中包括文献[35]中提到的缺少前向安全性以及相对低效(当下的方案需要对整个明文进行加密).所以,寻找前向安全的高效密码逆向防火墙方案,将成为日后的研究方向之一.

5 总结与展望

抗随机数后门攻击密码算法经过几年的研究,已经取得了一些有意义的成果.本文全方位地就其中的主要成果进行梳理总结,包括抗随机数后门攻击的对称加密算法、对冲公钥加密算法、基于随机性强化的方法以及其他相关技术目前的研究现状,分析了相关构造的特点,并指出目前相关技术研究过程中所面临的问题.总体来说,现有成果大多是从理论层面分析了抗随机数后门攻击的解决方案,而可实现的抗随机数后门攻击的密码算法仍然是需要进一步研究的主要方向.

现有的密码算法大多采用静态密码组件(如密钥生成器、PRNG 等)设计,这增加了算法在实现过程中被植入随机数后门的可能性.动态密码组件的使用,将能更有效地防止攻击者在算法中植入后门.例如,研究动态与交叉动态技术是未来抗随机数后门密码算法的一个研究方向:前者的基本思想在于对消息用多个动态变化的密码算法作用于该消息,并且其中的随机数生成算法使用不同的算法;后者的基本思想在于对多个动态变化的随机数生成算法产生的随机数进行一些运算(如异或等),将运算后的结果用于理论上安全的密码算法中.直观上,这两种技术可有效抵抗随机数后门攻击,然而如何对他们的安全性进行形式化分析还有待探讨.另外,目前抗随机数后门攻击密码算法的研究成果主要集中在加密算法方面,而在密钥协商协议、签名算法、签密算法等

方面的研究较少.因此,抗随机数后门攻击的密钥协商协议、签名算法、签密算法等方向都是未来的研究方向.最后,现有的抗随机数后门攻击密码算法大多数只能在随机预言模型下得到证明,在标准模型下可证明安全的抗随机数后门攻击密码算法为数不多.标准模型下,高效的抗随机数后门攻击密码算法还待进一步研究.

References:

[1] Bellare M, Tackmann B. Nonce-based cryptography: Retaining security when randomness fails. In: Fischlin M, Coron JS, eds. Proc. of the Advances in Cryptology (EUROCRYPT 2016). Berlin: Springer-Verlag, 2016. 729−757. [doi: 10.1007/978-3-662-49890-3_28]

[2] Boldyreva A, Patton C, Shrimpton T. Hedging public-key encryption in the real world. In: Katz J, Shacham H, eds. Proc. of the Advances in Cryptology (CRYPTO 2017). Berlin: Springer-Verlag, 2017. 462−494. [doi: 10.1007/978-3-319-63697-9_16]

[3] Huang Z, Lai J, Chen W, Au MH, Peng Z, Li J. Hedged nonce-based public-key encryption: Adaptive security under randomness failures. In: Abdalla M, Dahab R, eds. Proc. of the Public-key Cryptography (PKC 2018). Berlin: Springer-Verlag, 2018. 253−279. [doi: 10.1007/978-3-319-76578-5_9]

[4] Rogaway P. Nonce-based symmetric encryption. In: Roy B, Meier W, eds. Proc. of the Fast Software Encryption (FSE 2004). Berlin: Springer-Verlag, 2004. 348−358. [doi: 10.1007/978-3-540-25937-4_22]

[5] Dodis Y, Ganesh C, Golovnev A, Juels A, Ristenpart T. A formal treatment of backdoored pseudorandom generators. In: Oswald E, Fischlin M, eds. Proc. of the Advances in Cryptology (EUROCRYPT 2015). Berlin: Springer-Verlag, 2015. 101−126. [doi: 10.1007/978-3-662-46800-5_5]

[6] Zhang HG, Mao SW, Wu WQ, *et al*. Overview of quantum computation complexity theory. Chinese Journal of Computers, 2016,39(12):2403−2428 (in Chinese with English abstract).

[7] Shor PW. Polynomial-time algorithms for prime factorization and discrete logarithms on a quantum computer. SIAM Journal on Computing, 1997,26(5):1484−1509. [doi: 10.1137/S0097539795293172]

[8] Degabriele JP, Farshim P, Poettering B. A more cautious approach to security against mass surveillance. In: Leander G, ed. Proc. of the Fast Software Encryption (FSE 2015). Berlin: Springer-Verlag, 2015. 579−598. [doi: 10.1007/978-3-662-48116-5_28]

[9] Degabriele JP, Paterson KG, Schuldt JCN, Woodage J. Backdoors in pseudorandom number generators: Possibility and impossibility results. In: Robshaw M, Katz J, eds. Proc. of the Advances in Cryptology (CRYPTO 2016). Berlin: Springer-Verlag, 2016. 403−432. [doi: 10.1007/978-3-662-53018-4_15]

[10] Hoang VT, Katz J, O'Neill A, Zaheri M. Selective-opening security in the presence of randomness failures. In: Cheon J, Takagi T, eds. Proc. of the Advances in Cryptology (ASIACRYPT 2016). Berlin: Springer-Verlag, 2016. 278−306. [doi: 10.1007/978-3-662-53890-6_10]

[11] https://www.debian.org/security/2008/dsa-1571

[12] Heninger N, Durumeric Z, Wustrow E, *et al*. Mining your Ps and Qs: Detection of widespread weak keys in network devices. In: Proc. of the USENIX Security Symp., Vol.8. 2012. 1. [doi: 10.1179/026708401101517953]

[13] Fischlin M, Janson C, Mazaheri S. Backdoored Hash functions: Immunizing HMAC and HKDF. In: Proc. of the IEEE 31st Computer Security Foundations Symp. IEEE, 2018. 105−118. [doi: 10.1109/CSF.2018.00015]

[14] Auerbach B, Bellare M, Kiltz E. Public-key encryption resistant to parameter subversion and its realization from efficiently-embeddable groups. In: Abdalla M, Dahab R, eds. Proc. of the Public-key Cryptography (PKC 2018). Berlin: Springer-Verlag, 2018. 348−377. [doi: 10.1007/978-3-319-76578-5_12]

[15] Checkoway S, Niederhagen R, Everspaugh A, *et al*. On the practical exploitability of dual EC in TLS implementations. In: Proc. of the 23rd USENIX Security Symp. 2014. 319−335.

[16] Checkoway S, Maskiewicz J, Garman C, *et al*. A systematic analysis of the juniper dual EC incident. In: Proc. of the 2016 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2016. 468−479. [doi: 10.1145/2976749.2978395]

[17] Kamara S, Katz J. How to encrypt with a malicious random number generator. In: Nyberg K, ed. Proc. of the Fast Software Encryption (FSE 2008). Berlin: Springer-Verlag, 2008. 303−315. [doi: 10.1007/978-3-540-71039-4_19]

[18] Bellare M, Brakerski Z, Naor M, *et al*. Hedged public-key encryption: How to protect against bad randomness. In: Matsui M, ed. Proc. of the Advances in Cryptology (ASIACRYPT 2009). Berlin: Springer-Verlag, 2009. 232−249. [doi: 10.1007/978-3-642-10366-7_14]

[19] Bellare M, Boldyreva A, O'Neill A. Deterministic and efficiently searchable encryption. In: Menezes A, ed. Proc. of the Advances in Cryptology (CRYPTO 2007). Berlin: Springer-Verlag, 2007. 535−552. [doi: 10.1007/978-3-540-74143-5_30]

[20] Boldyreva A, Fehr S, O'Neill A. On notions of security for deterministic encryption, and efficient constructions without random oracles. In: Wagner D, ed. Proc. of the Advances in Cryptology (CRYPTO 2008). Berlin: Springer-Verlag, 2008. 335−359. [doi: 10.1007/978-3-540-85174-5_19]

[21] Rogaway P. Authenticated-encryption with associated-data. In: Proc. of the 9th ACM Conf. on Computer and Communications Security. ACM, 2002. 98−107. [doi: 10.1145/586110.586125]

[22] Rogaway P, Shrimpton T. A provable-security treatment of the key-wrap problem. In: Vaudenay S, ed. Proc. of the Advances in Cryptology (EUROCRYPT 2006). Berlin: Springer-Verlag, 2006. 373−390. [doi: 10.1007/11761679_23]

[23] Young A, Yung M. Kleptography: Using cryptography against cryptography. In: Fumy W, ed. Proc. of the Advances in Cryptology (EUROCRYPT'97). Berlin: Springer-Verlag, 1997. 62−74. [doi: 10.1007/3-540-69053-0_6]

[24] Young A, Yung M. The dark side of "black-box" cryptography or: Should we trust capstone? In: Koblitz N, ed. Proc. of the Advances in Cryptology (CRYPTO'96). Berlin: Springer-Verlag, 1996. 89−103. [doi: 10.1007/3-540-68697-5_8]

[25] Bellare M, Jaeger J, Kane D. Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2015. 1431−1440. [doi: 10.1145/2810103.2813681]

[26] Bellare M, Hoang VT. Resisting randomness subversion: Fast deterministic and hedged public-key encryption in the standard model. In: Oswald E, Fischlin M, eds. Proc. of the Advances in Cryptology (EUROCRYPT 2015). Berlin: Springer-Verlag, 2015. 627−656. [doi: 10.1007/978-3-662-46803-6_21]

[27] Bellare M, Paterson KG, Rogaway P. Security of symmetric encryption against mass surveillance. In: Garay JA, Gennaro R, eds. Proc. of the Advances in Cryptology (CRYPTO 2014). Berlin: Springer-Verlag, 2014. 1−19. [doi: 10.1007/978-3-662-44371-2_1]

[28] Russell A, Tang Q, Yung M, Zhou HS. Cliptography: Clipping the power of kleptographic attacks. In: Cheon J, Takagi T, eds. Proc. of the Advances in Cryptology (ASIACRYPT 2016). Berlin: Springer-Verlag, 2016. 34–64. [doi: 10.1007/978-3-662-53890-6_2]

[29] Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines. In: Robshaw M, Katz J, eds. Proc. of the Advances in Cryptology (CRYPTO 2016). Berlin: Springer-Verlag, 2016. 341−372. [doi: 10.1007/978-3-662-53018-4_13]

[30] Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Oswald E, Fischlin M, eds. Proc. of the Advances in Cryptology (EUROCRYPT 2015). Berlin: Springer-Verlag, 2015. 657−686. [doi: 10.1007/978-3-662-46803-6_22]

[31] Russell A, Tang Q, Yung M, *et al*. Destroying steganography via amalgamation: Kleptographically CPA secure public key encryption. Cryptology ePrint Archive: Report, 2016/530, 2016.

[32] Russell A, Tang Q, Yung M, *et al*. Generic semantic security against a kleptographic adversary. In: Proc. of the 2017 ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2017. 907−922. [doi: 10.1145/3133956.3133993]

[33] Lepinksi M, Micali S. Collusion-free protocols. In: Proc. of the 37th ACM Symp. on Theory of Computing. ACM, 2005. 543−552. [doi: 10.1145/1060590.1060671]

[34] Bellare M, Jaeger J, Kane D. Mass-surveillance without the state: Strongly undetectable algorithm-substitution attacks. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2015. 1431−1440. [doi: 10.1145/2810103.2813681]

[35] Mironov I, Stephens-Davidowitz N. Cryptographic reverse firewalls. In: Proc. of the Annual Int'l Conf. on the Theory and Applications of Cryptographic Techniques. Berlin: Springer-Verlag, 2015. 657−686.

[36] Prabhakaran M, Rosulek M. Rerandomizable RCCA encryption. In: Menezes A, ed. Proc. of the Advances in Cryptology (CRYPTO 2007). Berlin: Springer-Verlag, 2007. [doi: 10.1007/978-3-540-74143-5_29]

[37] Chen R, Mu Y, Yang G, Susilo W, Guo F, Zhang M. Cryptographic reverse firewall via malleable smooth projective Hash functions. In: Cheon J, Takagi T, eds. Proc. of the Advances in Cryptology (ASIACRYPT 2016). Berlin: Springer-Verlag, 2016. 844−876. [doi: 10.1007/978-3-662-53887-6_31]

[38] Groth J. Rerandomizable and replayable adaptive chosen ciphertext attack secure cryptosystems. In: Naor M, ed. Proc. of the Theory of Cryptography (TCC 2004). Berlin: Springer-Verlag, 2004. 152−170. [doi: 10.1007/978-3-540-24638-1_9]

[39] Ateniese G, Magri B, Venturi D. Subversion-resilient signature schemes. In: Proc. of the 22nd ACM SIGSAC Conf. on Computer and Communications Security. ACM, 2015. 364–375. [doi: 10.1145/2810103.2813635]

[40] Dodis Y, Mironov I, Stephens-Davidowitz N. Message transmission with reverse firewalls-secure communication on corrupted machines. In: Robshaw M, Katz J, eds. Proc. of the Advances in Cryptology (CRYPTO 2016). Berlin: Springer-Verlag, 2016. [doi: 10.1007/978-3-662-53018-4_13]

[41] Chen K. No place to hide: Edward Snowden, the NSA, and the US surveillance state. Journal of Intelligence and National Security, 2017,32(6):868–871. [doi: 10.1080/02684527.2016.1254142]

[42] Naor M, Pinkas B. Efficient oblivious transfer protocols. In: Proc. of the 12nd Annual ACM-SIAM Symp. on Discrete Algorithms. Society for Industrial and Applied Mathematics, 2001. 448–457.

附中文参考文献:

[6] 张焕国,毛少武,吴万青,等.量子计算复杂性理论综述.计算机学报,2016,39(12):2403–2428.

康步荣(1992－),女,博士生,主要研究领域为抗随机数后门攻击密码算法,车联网安全,云计算安全.

孟欣宇(1994－),女,博士生,主要研究领域为公钥密码学.

张磊(1982－),男,博士,研究员,博士生导师,主要研究领域为密码学,车联网安全,云计算安全,大数据安全,隐私保护.

陈桐(1996－),男,硕士,主要研究领域为网络安全,区块链.

张蕊(1996－),女,博士生,主要研究领域为交互式多方安全计算.