计算机研究与发展
Journal of Computer Research and Development
DOI:10.7544/issn1000-1239.2017.20170422
54(10):2244-2254,2017

基于强变色龙 Hash 函数的紧致安全签名通用构造

李 飞[1,2] 高 伟[1,2] 王贵林[3] 谢冬青[2] 唐春明[2]
[1](鲁东大学数学与统计科学学院 山东烟台 264025)
[2](广东省信息安全技术重点实验室(广州大学) 广州 510006)
[3](华为新加坡研究所谢尔德实验室 新加坡 117674)
(miss_lifei@163.com)

Generic Tightly Secure Signature Schemes from Strong Chameleon Hash Functions

Li Fei[1,2], Gao Wei[1,2], Wang Guilin[3], Xie Dongqing[2], and Tang Chunming[2]
[1](*School of Mathematics and Statistics, Ludong University, Yantai, Shandong* 264025)
[2](*Guangdong Provincial Key Laboratory of Information Security Technology (Guangzhou University), Guangzhou* 510006)
[3](*Shield Laboratory, Singapore Research Center of Huawei, Singapore* 117674)

Abstract Provable security has become one basic requirement for constructing and analyzing cryptographic schemes. This paper studies the classical issue in the field of provable security, namely how to construct provably secure digital signature schemes with tight security reduction from certain basic mathematical hard problems in the random oracle model. This paper first proposes a new cryptographic primitive called a strong chameleon Hash function. Based on a strong chameleon Hash function, we present a generic framework and its variant respectively for constructing a stateful and stateless digital signature scheme with tight security. We prove that these generic digital signature schemes are both secure under the assumption that the underlying chameleon Hash function is collision resistant in the random oracle model. By applying these generic construction methods to some concrete chameleon Hash functions under common mathematical assumptions such as RSA, CDH and IF (integer factorization), the corresponding digital signature schemes with tight security can be modularly obtained. The two existing classic paradigms to generically construct tightly secure signature schemes, i.e. Fiat-Shamir signatures and Full-Domain-Hash signatures, can be roughly unified by our generic frameworks. Furthermore, under our generic frameworks, a tightly secure signature scheme following the Fiat-Shamir methodology can be seen as the optimized variant of the corresponding tightly secure signature scheme following the Full-Domain-Hash framework.

Key words digital signature; provable security; tight security; random oracle model; chameleon Hash function; full domain Hash signature

摘 要 可证明安全性已经成为构造和分析密码方案的一个基本要求.研究可证明安全密码学领域的一个经典问题,即如何在随机预言模型下构造可证明安全的数字签名方案,而且其安全性可紧致地规约为

收稿日期:2017-06-10;**修回日期**:2017-07-28
基金项目:国家自然科学基金项目(61202475);广东省信息安全技术重点实验室开放课题(GDXXAQ2016-02);山东省统计科研重点课题(KT16022);鲁东大学博士人才科研基金项目(2017)
This work was supported by the National Natural Science Foundation of China (61202475), the Open Project of Guangdong Provincial Key Laboratory of Information Security Technology (GDXXAQ2016-02), the Shandong Provincial Statistics Key Project (KT16022), and the Ludong University Research Foundation for Doctoral Talents (2017).

某个基础数学问题的困难性.首先提出一种新密码原型,称作强变色龙 Hash 函数;然后基于强变色龙 Hash 函数,给出紧致安全数字签名方案的一般化构造框架及其变形,分别对应带状态和无状态 2 种情形;接着证明了这 2 种通用方案的安全性均可规约为底层强变色龙 Hash 函数的抗碰撞性.利用 RSA,CDH,IF 等具体假设下的强变色龙 Hash 函数,通过所提出的一般化构造技术,可以模块化地构造相应的具体的紧致安全签名方案.2 类经典的紧致安全签名方案构造范式,即 Fiat-Shamir(FS)类和 Full-Domain-Hash(FDH)类,可大致统一在所提出的构造框架中,而且本框架可将 FDH 类紧致安全签名方案解释为相应 FS 类紧致签名方案的优化形式.

关键词　数字签名;可证明安全;紧致安全性;随机预言模型;变色龙 Hash 函数;全域 Hash 签名

中图法分类号　TP309

在现代密码学中具备可证明安全性[1]是公钥加密[2]、数字签名[3]、密钥交换[4]等公钥密码方案设计的最基本原则之一.紧致安全性则是可证明安全性要求的进一步提升[1].本文力图发展一种新的通用框架,可以基于某种底层困难问题通过模块化方式构造紧致安全的数字签名方案,代替传统的仅能实现松散安全性归约的先 Hash 后求逆的构造签名框架.进一步地,这个框架所基于的底层困难问题应该是一个非常基础且具有高度概括性的密码原型,最好是能在陷门置换的基础上增加一些最必要的密码学性质,而这些密码学性质恰恰又是使得安全性证明达到紧致要求的必要条件.事实上,这就是本文所提出一种新型密码原型,称作强变色龙 Hash 函数.本文结合实例作了相关比较及分析,从而说明本文所给出的紧致安全签名的一般性构造框架具有高度概括性,既可导出具体的 FDH 类[5]紧致安全签名方案,又可导出具体的 FS 类[6]紧致安全签名方案.特别值得注意是,FDH 类签名方案和 FS 类签名方案,在密码学的相关研究领域中通常被认为是 2 类相互独立的一般性签名构造框架.本文结果表明,至少在紧致安全签名构造方面,二者是统一的:本文的统一框架下,FDH 紧致签名方案基本可以看作是对应的 FS 类签名方案的优化结果.

本文的主要贡献包括 3 个方面:

1) 作为理论基础,本文提出了一种新的密码原型,称作强变色龙 Hash 函数,既可以看作经典变色龙 Hash 函数概念的推广,又可看作陷门置换的推广,从而兼具这 2 种重要密码原型的基本密码性质.特别需要指出的是,强变色龙 Hash 函数的可逆性在传统变色龙 Hash 函数的相关研究中极少提到,这主要是因为变色龙 Hash 函数的原有应用环境只是需要该密码原型的抗碰撞性和"变色龙"性质.然而强变色龙 Hash 函数的可逆性在本文签名方案的构造中起到了不可或缺的基础性作用.

2) 本文提出一种可证明安全签名方案的一般性构造框架,而且安全性归约达到了紧致性要求.这个基础型可证明安全签名框架是带状态的,即要求签名者记录所有签名历史,避免对同一个消息产生 2 种不同的签名.因此,本文给出了这种一般性签名方案的改进方法,可以非常容易地实现不带状态的紧致安全签名方案.

3) 作为上述一般性签名框架的应用,本文以基于 RSA 的签名方案为例,给出了 3 个紧致安全的 RSA 签名方案,并将这些具体签名方案与现有的 FS 类和 FDH 类签名方案进行比较,从而表明以上理论框架可以导出 FS 类签名方案和 FDH 类签名方案,其技术水平与直接构造的同类紧致安全签名方案持平.同时,这一理论结果也在某种程度上"否定"了 FS 类紧致安全签名方案的构造,这是因为在本文的理论框架下,FDH 类签名方案可以看作对应 FS 类数字签名方案的优化结果.

1　研究背景与相关工作

1988 年,Goldwasser 等人[7]以形式化方式给出了数字签名的经典定义,此定义使用了渐进安全性(asymptotic security)的描述方法:所谓一个安全性证明就是一个归约算法,它调用一个多项式时间复杂度的签名伪造算法构造出一个解决底层困难问题的多项式时间算法,进而由反证法得出安全性证明.渐进安全性证明在理论上讲是很好的,但是其实际应用却存在很大局限.当需要评估一个数字签名方案在给定的具体安全参数和具体攻击资源等条件下的实际安全性时,渐进安全性就不再适用.

受实际应用环境对数字签名安全强度精确化要求的驱动,Bellare 和 Rogaway[5]在 1996 年提出了具体安全性(concrete security)的概念,其特点是力

图给出伪造签名的困难程度与解决底层数学问题的困难程度之间的精确关系.在具体安全性框架下,可以进一步考虑安全归约的紧致性(tightness).在文献[8]中提到,如果伪造签名的难度与攻击底层数学问题的难度非常接近,则称该归约是紧致的,否则称该归约是松散的.换句话说,对于紧致安全归约来说,签名伪造算法的成功概率和运行时间与解决底层困难问题的成功概率和运行时间可看作是大致相同.通过本文后面所给数字签名方案的安全性归约,可以更加具体地认识和理解安全性归约的"渐进"、"具体"、"紧致"、"松散"等抽象概念的含义.

就数字签名方案的安全性证明是否依赖随机预言假设,可证明安全数字签名方案可分为随机预言模型下安全类和标准模型下安全类.所谓随机预言假设[9]是在密码方案的安全性证明中,把某个密码学意义下 Hash 函数理想化为一个完全随机函数,也就是假设存在一个各方均可访问的随机预言机,对于每次询问所返回的 Hash 值都是完全随机的,而且同一个数值的 Hash 值总是相同的.通常认为,Hash 函数仅有抗碰撞性,随机预言模型假设该函数具有完全随机性,而函数的随机性是密码学对函数性质的最高要求,可见随机预言假设是一个非常强的假设.因此,在可证明安全密码学研究领域,有一派研究是致力于标准安全密码方案的构造.目前,人们已经构造了不少标准模型下安全的数字签名方案,例如文献[10-13]所给出的签名方案.与随机预言模型下安全的数字签名方案相比,这些标准安全的数字签名方案往往效率较低,实际应用中受到很大限制.本文主要考虑随机预言模型下安全数字签名的构造问题,重点关注这些签名方案安全性归约的紧致性.随机预言模型下安全的数字签名方案基本分为 2 类:

1) FDH 类,即全域 Hash 类签名方案基本都是按照以下框架构造的.令 f 是一个陷门置换函数,其陷门(即函数 f 的逆变换)记作 f^{-1}.令 RO 是一个随机预言机,可将定义域 $\{0,1\}^*$ 的值映射到函数 f 的值域中的一个随机值.对于全域 Hash 签名方案[5,9],消息 m 的签名形式为 $\sigma=f^{-1}(RO(m))$,其签名验证是看等式 $f(\sigma)=RO(m)$ 是否成立.令 (ε,t) 分别是伪造签名算法的成功概率和运行时间,而 (ε',t') 分别是解决底层困难问题的算法的成功概率和运行时间,这里解决底层问题的算法即是安全性证明的归约算法,是调用签名伪造算法作子函数来构造的.对于一个可证明安全数字签名方案及其安全归约来说,所谓归约(或者说安全性)紧致通常是指 $\varepsilon\approx c_1\varepsilon'$, $t\approx c_2 t'$,其中 c_1, c_2 均是较小常数.所谓归约松散,往往是指这些系数是归约算法中某些参数的函数,如系数是敌手访问随机预言机次数的二次多项式.系数 c_1, c_2 有时称作(概率、时间)紧致系数.

当陷门置换函数 f 是 RSA 函数时,即 $f(x)=x^e \bmod n$,得到了具体的 FDH 签名方案,记作 RSA-FDH.对于 RSA-FDH,Bellare 和 Rogway[5]在 1996 年分析了具体安全性,但是所给出归约非常松散,即 $t\approx t'$, $\varepsilon\approx(q_s+q_h)\varepsilon'$,此处,$q_s$ 和 q_h 分别表示在定义安全性的游戏过程中敌手所作签名询问次数和随机预言机询问次数.2000 年,Coron[14]给出了更加紧致的安全性归约(也就是更加紧致的安全性证明),所给出的概率关系式为 $t\approx t'$, $\varepsilon\approx q_s\varepsilon'$,即系数中不再含有随机预言机访问次数 q_h.其安全性归约的紧致性得以提升的关键是利用了 RSA 函数的随机自归约性质(random self-reducibility)[15].为了进一步提升归约紧致性,即去掉上式系数中的 q_s,Bellare 和 Rogway[5]提出 RSA-FDH 签名方案的一种改进形式,称作 PSS,并指出其安全性归约是紧致的,即 $\varepsilon\approx\varepsilon'$.文献[5]的核心思想是对签名过程进行随机化,即在签名中引入一个随机因子 r.在 2002 年,Coron[16]作了进一步分析,在保证归约紧致性基本不变的情况下,可以进一步优化随机因子 r 的长度.2002 年,Dodis 和 Reyzin[15]对以上结果进行了系统的理论化整理,所依赖的基本密码原型为无爪置换(claw-free permutations):

① 如果作为构建模块的陷门置换函数 f 仅仅是一个黑盒形式的陷门置换,即仅考虑函数的陷门性质,不考虑其他具体的特殊性质,如文献[14-15]所提到的 RSA 函数的随机自归约性,那么相应的 FDH 签名所能达到的归约紧致性只能是 $\varepsilon\approx(q_s+q_h)\varepsilon'$.

② 如果陷门函数 f 可以看作是无爪置换所诱导的,那么 FDH 签名的归约紧致性可以进一步优化为 $\varepsilon\approx q_s\varepsilon'$.

③ 在陷门函数 f 由无爪置换诱导,且签名中引入随机因子 r 的情况下,随机化后的 FDH 签名的归约紧致性可以再进一步优化为 $\varepsilon\approx\varepsilon'$,此时的签名形式为 $\sigma=(f^{-1}(RO(m,r)),r)$.

2003 年,Katz 和 Wang[17]改进了 FDH 类签名方案,其改进后的签名形式为 $\sigma=(f^{-1}(RO(m,b)),b)$,其归约紧致性基本达到最优,即 $\varepsilon\approx\varepsilon'$,而随机因子 b

只需 1 比特.其代价是:所给的基础签名方案是带状态的,即需要签名者记录所有已经签过的消息及签名,以免对同一个消息产生 2 个不同的签名.同时,他们还给出了一般性转换方法,可以将此带状态的签名方案转换为不带状态形式.

借鉴以上基于陷门置换构造 FDH 类签名方案的思想及实现紧致安全性的技术框架,基于 BLS 短签名[18],同样可以构造出相应的变形方案且实现紧致安全性[17].值得注意的是 BLS 签名及其紧致安全的变形方案所依赖的底层困难问题是 CDH 假设,这并不是陷门置换.如何给出一个比陷门置换更具概括性的密码原型,并进一步扩展类似于随机自归约的性质,并分析这些性质与紧致归约之间的理论联系是紧致安全签名方案构造理论的一个重要方面,也是本文的一个理论性目标.

2) FS 类签名方案开始于 Fiat 和 Shamir[6],可以看作是与 FDH 类签名并列的另外一种签名构造框架.FS 类签名包括了基于离散对数的签名方案,而离散对数问题并不存在陷门.前面介绍的 FDH 类签名所依托的困难问题则必须有陷门.下面首先给出 FS 类签名的一般性构造框架.

一个经典身份认证方案由 3 个操作过程构成:

步骤 1.证明方发送承诺值 Y 给验证方,通常 Y 的计算需要用到保密的随机串 y;

步骤 2.验证方发送随机选取的一个足够长度的挑战值 c 给验证方;

步骤 3.证明方利用其私钥及之前的内部随机信息 y 计算并发送一个应答值 z 给验证方,验证方检验对话副本 (Y,c,z) 是否合法.

利用 Fiat-Shamir 转换[6,19],以上形式的经典身份认证方案可以转化为数字签名方案.所得签名形式为 (Y,z),而验证 (Y,z) 是否合法只需判断 $(Y,c=H(Y,m),z)$ 是否通过协议验证算法.此处 H 为密码学意义下的 Hash 函数,在安全性证明时作为随机预言机对待.一方面,通过 Fiat-Shamir 转换框架,构造了一批高效的签名方案.另一方面,在安全性归约的紧致性方面,此类签名方案往往仅能达到较为松散的安全性归约,这是此类签名方案的主要不足之处.进一步地,安全性归约松散的根本原因在于安全性归约对于所谓的分叉引理[20]的依赖.事实上,对于 FS 类签名方案的安全性,令 ε 是伪造签名算法的成功概率,ε' 是解决底层困难问题的成功概率(对于著名的 Schnorr 签名来说[19,21],底层困难问题是 DLP 问题),q_h 是敌手访问随机预言机的次数,则有 $\varepsilon \approx q_h \sqrt{\varepsilon'}$.因此,Fiat-Shamir 类签名的安全性归约通常是松散的,这也引起了人们研究 FS 类签名的紧致性安全归约的热情.

1999 年,Micali 和 Reyzi[8] 提出了一种称作 SWAP 的通用型转化框架,可以模块化地构造具有紧致安全性的 FS 类签名方案.SWAP 转换框架与以上 Fiat-Shamir 转换框架在形式上类似,可看作 Fiat-Shamir 转换的变形,因此也将其归为 FS 类签名.SWAP 转换框架对于底层的典型身份认证方案提出了特殊要求:证明方在不需要知晓 y(计算承诺时所选择的随机秘密值)的条件下,可以直接由承诺 Y 和挑战 c 计算出应答值 z.在 SWAP 转换框架中,签名形式为 (c,z).若 (Y,c,z) 是合法的协议副本,则 (c,z) 就是合法签名,此处 $Y=H(c,m)$,H 是密码学意义下的 Hash 函数(在安全性证明中需理想化为随机预言机).Micali 和 Reyzin[8] 利用 SWAP 转换构造了一种基于整数分解难题的签名方案,其安全性归约关系为 $\varepsilon \approx \varepsilon'$,其中 ε' 表示归约算法解决整数分解问题的成功概率.

2016 年,Abdalla 等人[22] 提出了所谓的损耗性身份认证方案,并证明了针对这类损耗性身份认证方案应用 Fiat-Shamir 转换,可以得到紧致安全的数字签名方案.分别基于理想格上的最短向量问题、c 确定型离散对数问题(c-decisional discrete logarithm)和子集和问题(subset sum)等数学难题,Abdalla 等人给出 3 种具体的损耗性身份认证方案[22]及对应的紧致安全签名方案.大致来说,在一个损耗性身份认证方案中,证明方的公钥可以采用 2 种不可区分形式中的任何一种,分别称为正常型(normal)和损耗型(lossy).对于文献[22]所给出的数字签名方案来说,安全性归约的关系式表示为 $\varepsilon \approx \varepsilon'$,此处 ε' 是敌手成功攻破损耗性身份认证方案的密钥不可区分性质的概率,ε 仍然是伪造签名算法的成功概率,可见此类签名方案也达到了紧致安全性.值得注意的是,一般来说,损耗性身份认证方案的密钥不可区分性质往往与确定性(decisional)困难问题相关.从这类签名所依赖的具体困难问题来看,其应用范围具有很大限制性.

2016 年 Bellare 等人[23]研究了由身份认证方案到紧致安全签名的一般化构造框架,这是 FS 转换框架的改进模式.Bellare 等人首先给出了身份认证方案的安全性定义框架,而这一框架又细分出 4 种具体形式,然后给出了 3 种 FS 类转换框架并分析、比较了这些框架的相关指标.需要指出的是身份认证

方案并不是最底层的密码方案,其安全性定义及安全性分析是非常复杂的.从密码学理论角度看,把紧致安全签名方案的构造归为某类更加简练的密码原型的构造(例如作为一种底层构造模块,本文给出的强变色龙 Hash 函数就比身份认证方案更为简练)是需要进一步研究的理论课题.

另外,Goh 和 Jarecki 在 2003 年提出了一种基于 CDH 困难问题的 FS 类签名方案[24],之后针对该方案又作了进一步的改进[25].这 2 个 FS 类签名方案的安全性归约均基本达到了最优紧致性,即 $\varepsilon \approx \varepsilon'$,此处 ε' 是归约算法解决 CDH 困难问题的成功概率,而 ε 仍然是伪造签名算法的成功概率.在文献[17]中,Katz 和 Wang 还提出了一种基于 DDH 困难问题 (decisional Diffie-Hellman) 的 FS 类签名,其安全性可紧致地归约为 DDH 问题的困难性,在签名长度和计算效率方面均优于文献[24-25]所给的基于 CDH 困难问题的 FS 类签名方案.

2 预备知识

本节介绍数字签名语法定义及安全性定义[5,7].

定义 1. 一个数字签名方案

$$DS=(S.Gen,S.Sign,S.Vrf)$$

由 3 个概率多项式时间算法组成:

1) $(pk,sk)\leftarrow S.Gen(1^{\lambda})$.这是密钥生成算法.输入安全参数 1^{λ},输出公钥 pk 和私钥 sk.

2) $\sigma\leftarrow S.Sign(sk,m)$.这是数字签名生成算法.输入待签名消息 m 和私钥 sk,输出签名 σ.

3) $b\leftarrow S.Vrf(pk,m,\sigma)$.这是数字签名验证算法.输入消息 m、签名 σ 和公钥 pk,输出一个比特 b,表示 σ 是否合法.

定义 2. 称一个数字签名方案在选择消息攻击下是 (t,ε) 不可伪造的,如果对于任何的运行时间不超过 t 的伪造者 $\mathcal{A}$,下述概率不等式总成立:

$$Pr[S.Vrf(pk,m^*,\sigma^*)=1\wedge m^*\notin S^* \mid (sk,pk)\leftarrow_{R} S.Gen(1^k);(\sigma^*,m^*)\leftarrow_{R}\mathcal{A}^{O^{Sign}()}(pk)]<\varepsilon,$$

此处 S^* 表示伪造者已经索得签名的所有消息集合,即不存在伪造算法满足运行时间小于等于 t,成功概率大于等于 ε.

3 强变色龙 Hash 函数

本节提出强变色龙 Hash 函数的定义,并给出 3 个具体方案.

3.1 强变色龙 Hash 函数定义

定义 3. 一个强变色龙 Hash 函数(族):

$$SCH=(H.Gen,H.Hash,H.Ivt)$$

由 3 个概率多项式时间算法组成:

1) $(hk,itd)\leftarrow H.Gen(1^{\lambda})$.该算法为密钥生成算法,其输入为安全参数 λ,其输出是 Hash 密钥 hk 和求逆陷门 itd.Hash 密钥 hk 决定了消息集合 $\mathcal{S}$、随机种子集合 $\mathcal{R}$ 和 Hash 值集合 $\mathcal{H}$.每个 Hash 密钥都确定了变色龙 Hash 函数(族)中的一个具体变色龙 Hash 函数.在不产生歧义的情况下,一个 Hash 函数可以指一个 Hash 函数族,也可以指一个具体的 Hash 函数.

2) $(h,r)\leftarrow H.Hash(hk,s)$.该算法为强变色龙 Hash 函数的 Hash 算法.对于待 Hash 消息 $s\in_{R}\mathcal{S}$ 及 Hash 密钥 hk,选择一个随机数 $r\in_{R}\mathcal{R}$,然后计算 Hash 值 $h\leftarrow \mathrm{Hash}_{hk}(s,r)\in\mathcal{H}$,最后返回 Hash 值及随机种子 (h,r).此处,明确区分了随机化算法 $H.Hash(hk,s)$ 和确定算法 $\mathrm{Hash}_{hk}(s,r)$.二者本质上没有区别,只是为了相关叙述的方便.

3) $r\leftarrow H.Ivt(hk,itd,h,s)$.此算法称作强变色龙 Hash 函数的求逆算法.对于给定的 Hash 值 h 和被 Hash 消息 s,该算法计算随机种子 $r\in_{R}R$ 使得 $h=\mathrm{Hash}_{hk}(s,r)$.该算法的存在性正是强变色龙 Hash 函数的"强变色性"的形式化描述.也就是说,借助陷门 itd,该算法能够提供相应的随机值 r,从而可以将任意 Hash 值 h 解读为任意消息 s 的 Hash 值,特别是此时不需要知道 h 的另外原象.

抗碰撞性:称强变色龙 Hash 函数(族)是抗碰撞的,如果对于任何运行时间不超过的概率多项式时间敌手 $\mathcal{A}$,下面过程的成功概率总满足:

$$Pr[\mathrm{Hash}_{hk}(s,r)=\mathrm{Hash}_{hk}(\hat{s},\hat{r})\wedge(s,r)\neq(\hat{s},\hat{r}) \mid (hk,itd)\leftarrow_{R} H.Gen(1^{\lambda});(s,r),(\hat{s},\hat{r})\leftarrow\mathcal{A}(hk)]<\varepsilon,$$

即不存在碰撞算法满足运行时间小于等于 t,成功概率大于等于 ε.

为了更好地理解这一新概念,对于上述形式化定义,下面分析强变色龙 Hash 函数与其他相关密码学概念之间的关系.

1) 强变色龙 Hash 函数和传统变色龙 Hash 函数[26]二者之间的关系.对于强变色龙 Hash 函数来说,其陷门可以用来对任意的 Hash 值 h,求出原象对 (s',r');而对于传统变色龙 Hash 函数来说,其陷门可以用来对任意的原象对 (s,r),求出第二原象对 (s',r').换句话说,用强变色龙 Hash 函数的陷门可

以任意求逆(从多个符合条件的原象中,选择一个),而传统变色龙 Hash 函数,其陷门可以计算碰撞.通常,求逆算法必定可以平凡地导出求碰撞算法,反之则不然.因此,以上定义称为强变色龙 Hash 函数.需要特别指出的是,有些具体的变色龙 Hash 函数本身也是强变色龙 Hash 函数,但是当时应用环境并未牵涉到"强"变色性,因此并未明确提出该性质.

2) 作为一种底层的密码原型概念,强变色龙 Hash 函数可以看作陷门单向函数概念的拓展.事实上,在函数 $\mathrm{Hash}_{hk}(s,r)$ 和 $H.Ivt(hk,itd,h,s)$ 中固定变量 s,将会自然诱导出一个陷门单向函数 f 及其逆函数 g:

$$f_{hk,s}(r)=\mathrm{Hash}_{hk}(s,r),r\in\mathcal{R},$$

$$g_{hk,s,itd}(h)=H.Ivt(hk,itd,h,s),h\in\mathcal{H}.$$

3) 作为一种基础密码原型,强变色龙 Hash 函数可以看作无爪置换(claw-free permutations)[15]的一种扩展.事实上,对于函数 $\mathrm{Hash}_{hk}(s,r)$,分别给变量 s 不同的赋值 $s=s_0$,$s=s_1$,将会自然诱导出相应的一对函数:

$$f_{hk,s_0}(r)=\mathrm{Hash}_{hk}(s_0,r),r\in\mathcal{R},$$

$$f_{hk,s_1}(r)=\mathrm{Hash}_{hk}(s_1,r),r\in\mathcal{R}.$$

对于上述函数对,根据抗碰撞性质,计算 r_0,r_1 使得 $f_{hk,s_0}(r_0)=f_{hk,s_1}(r_1)$ 在计算上是不可行的.从而,$\{(f_i:\mathcal{R}\to\mathcal{H},g_i:\mathcal{R}\to\mathcal{H})\mid f_i(r)=f_{hk,s_0}(r),f_i(r)=f_{hk,s_1}(r),r\in R\}$构成了一个无爪置换族[15].简言之,无爪置换族是强变色龙族 Hash 函数的简化形式.特别地,当 s 的取值集合 $\mathcal{S}$ 只有 2 个元素,自然得出无爪置换族.

3.2　强变色龙 Hash 函数的具体方案

本节给出强变色龙 Hash 函数的 3 个具体构造,分别基于 CDH,RSA 和 IF 等常见困难问题.通过这些具体构造,容易得出初步结论:

1) 从刻划密码学概念的角度来讲,强变色龙 Hash 函数是对传统变色龙 Hash 函数的加强,而且强化后的性质将在后续签名方案构造中发挥重要作用.

2) 从方案构造角度来说,以往的某些变色龙 Hash 函数本身具有"强变色"的性质,只是由于缺乏该性质的应用背景驱动,而没有提出"强变色"性质的抽象概念.

本节只是给出函数的方案描述,各相关性质易于验证,其证明不作赘述.

3.2.1　*SCH-CDH*:基于双线性对的强变色龙 Hash 函数构造

根据文献[27]中基于双线性对的无密钥泄漏变色龙 Hash 函数,容易得出强变色龙 Hash 函数:

1) $H.Gen(1^\lambda)$.选取 2 个乘法群 G,G_T 及相关双线性对 $e:G\times G\to G_T$,随机选择 $\alpha,\beta\leftarrow_R\mathbb{Z}_q$,并计算 $\bar{g}=g^\alpha$,其中 $G=\langle g\rangle$,$|G|=q$,q 是素数.令 Hash 密钥和求逆陷门为

$$hk=(g,g^\alpha,g^\beta),$$

$$itd=\alpha.$$

2) $H.Hash(hk,s)$.对于给定的 Hash 密钥 $hk=(g,g^\alpha,g^\beta)$,待 Hash 消息 $s\in\mathbb{Z}_q$,随机选择 $\gamma\leftarrow_R\mathbb{Z}_q$,并计算 $r=(g^{\alpha\gamma},g^\gamma)$,然后计算 Hash 值:

$$h=\mathrm{Hash}_{g,g^\alpha,g^\beta}(s,r)=(g^\beta)^s g^\gamma.$$

之后返回 Hash 值 h 及随机信息 $r=(g^{\alpha\gamma},g^\gamma)$.只有当 $h=(g^\beta)^s g^\gamma$ 和 $e(g,r')=e(r'',g^\alpha)$(此式用于保证的确存在 γ 使得 $r=(r',r'')=(g^{\alpha\gamma},g^\gamma)$)同时成立时,才认为 h 为 s 的 Hash 值.

3) $H.Ivt(hk,itd,h,s)$.对于给定的 Hash 值 h 和被 Hash 消息 s,计算:

$$r''=h(g^\beta)^{-s},$$

$$r'=r''^{\alpha}.$$

最后输出 $r=(r',r'')$.输出值的正确性为

$$\mathrm{Hash}_{g,g^\alpha,g^\beta}(s,r)=(g^\beta)^s g^\gamma=(g^\beta)^s h(g^\beta)^{-s}=h,$$

$$e(g,r')=e(r'',g^\alpha).$$

3.2.2　*SCH-RSA*:基于 *RSA* 困难问题的强变色龙 Hash 函数构造

根据文献[28]中基于 RSA 的无密钥泄漏变色龙 Hash 函数,容易得出强变色龙 Hash 函数:

1) $H.Gen(1^\lambda)$.根据输入的安全参数 λ,选择同样长度的不同素数 p,q,并计算 $n=pq$;然后,选择足够大的素数 $e>l$,此处参数 l 保证 e 足够大;接着计算 d,使得 $ed=1 \bmod (p-1)(q-1)$;最后,随机选择 $x\leftarrow_R\mathbb{Z}_q$,并计算求逆陷门和 Hash 密钥:

$$itd=d,$$

$$hk=(n,e,x^e).$$

2) $H.Hash(hk,s)$.给定 Hash 密钥 hk 和被 Hash 消息 $s\in\mathbb{Z}_e$,该算法选择 $r\leftarrow_R\mathbb{Z}_n^*$,计算 Hash 值为

$$h=\mathrm{Hash}_{hk}(s,r)=(x^e)^s r^e \bmod n.$$

之后,返回 Hash 值及随机信息(h,r).

3) $H.Ivt(hk,itd,h,s)$.对于给定的 Hash 值 h 和被 Hash 消息 s,利用陷门信息 $itd=d$,计算随机种子:

$$r=(h(x^e)^{-s})^d \bmod n.$$

该输出值的正确性为

$$\mathrm{Hash}_{hk}(s,r)=(x^e)^s r^e \bmod n=$$

$$(x^e)^s(h(x^e)^{-s})^{de} \bmod n=h \bmod n.$$

3.2.3 *SCH-IF*：基于整数分解难题的强变色龙 Hash 函数构造

根据文献[29]中基于 IF 的无密钥泄漏变色龙 Hash 函数，容易得出强变色龙 Hash 函数：

1) $H.Gen(1^\lambda)$. 首先随机选择同样长度的不同素数 p,q，使得 $p,q=3 \bmod 4$，计算 $n=pq$，确定一个辅助的整数型参数 τ. 如此形式的 RSA 模 n 通常称作 Blum-Williams 整数或 Blum 整数[1,23]. 随机选择 $x\in QR_n$，令 Hash 密钥 hk 和求逆陷门 itd 分别为

$$hk=(n,\tau,x^{2^\tau}),itd=(p,q).$$

2) $H.Hash(hk,s)$. 给定待 Hash 消息 $s\in_R\mathbb{Z}_{2^\tau}$ 和 Hash 密钥 hk，随机选择 $r\leftarrow_R\mathbb{Z}_n^*$，然后计算 Hash 值：

$$h=\mathrm{Hash}_{hk}(s,r)=(x^{2^\tau})^s r^{2^\tau} \bmod n.$$

之后，输出 Hash 值 h 及随机信息 r.

3) $H.Ivt(hk,itd,h,s)$. 对于 Hash 值 h 和被 Hash 消息 s，该算法利用陷门信息 $itd=(p,q)$，计算与之对应的随机信息：

$$r=(h\times(x^{2^\tau})^{-s})^{1/2^\tau} \bmod n.$$

该输出值的正确性为

$$\mathrm{Hash}_{hk}(s,r)=(x^{2^\tau})^s r^{2^\tau} \bmod n=$$
$$(x^{2^\tau})^s(h(x^{2^\tau})^{-s})^{1/2^\tau\cdot 2^\tau} \bmod n=h \bmod n.$$

4 带状态的紧致安全签名方案

本节提出由强变色龙 Hash 函数构造紧致安全签名方案的 2 种一般性框架，分别对应带状态和不带状态 2 种情形，并在随机预言模型下分析其紧致安全性.

4.1 带状态的紧致安全签名方案

给定任意一个强变色龙 Hash 函数族 $SCH=(H.Gen,H.Hash,H.Ivt)$，可以构造如下带状态的数字签名方案，记作 *SCH-2-DS*0：

1) $S.Gen(1^\lambda)$. 首先，运行强变色龙 Hash 函数的密钥生成算法 $(hk,itd)\leftarrow_R H.Gen(1^\lambda)$，令签名公钥和私钥分别为

$$pk=hk,$$
$$sk=itd.$$

设 $\mathcal{S},\mathcal{R},\mathcal{H}$ 分别为强变色龙 Hash 函数族的被 Hash 消息集合、随机种子集合和 Hash 值集合. 再取子集 $\hat{\mathcal{S}}\subset\mathcal{S}$ 作为公开参数，要求 $\hat{\mathcal{S}}$ 至少含有 2 个元素. 另外，选定一个密码学意义下的 Hash 函数 $H_1:\mathcal{M}\to\mathcal{H}$ 作为公开参数，此处 $\mathcal{M}$ 是待签名消息的集合.

2) $S.Sign(sk,m)$. 对于待签名的消息 $m\in\mathcal{M}$，首先检查该消息是否已经签过. 如果是，则返回之前的签名；否则，根据签名的公钥 $pk=hk$ 和私钥 $sk=itd$，计算

$$h\leftarrow H_1(m),$$
$$s\leftarrow_R\hat{\mathcal{S}},$$
$$r\leftarrow H.Ivt(hk,itd,h,s).$$

然后返回签名 $\sigma\leftarrow(s,r)$. 同时，记录此次的消息及其签名. 注意，每次签名前需要检查之前的签名，且在签名后作记录，就是所谓的带状态性(stateful). 简言之，该签名方案就是对消息的普通 Hash 值进行变色龙 Hash 函数的求逆. 这种数字签名构造框架与最通常的 Full-Domain-Hash 签名[9,14]非常相似.

3) $S.Vrf(pk,m,\sigma)$. 对于给定的公钥 $pk=hk$，验证 $\sigma=(s,r)$ 是否为消息 m 的合法签名，即验证是否成立：

$$H_1(m)=\mathrm{Hash}_{hk}(s,r).$$

定理 1. 如果底层的强变色龙 Hash 函数 $SCH=(H.Gen,H.Hash,H.Ivt)$ 是 (t',ε') 抗碰撞的，那么上述签名方案：

$$SCH\text{-}2\text{-}DS0=(S.Gen,S.Hash,S.Vrf)$$

就是 (t,ε) 存在性不可伪造的，其中：

$$\varepsilon'=(1-\frac{1}{|\hat{\mathcal{S}}|})\varepsilon,$$
$$t'=t+q_{\mathrm{Hash}}\times t_{\mathrm{Hash}},$$

其中，q_{Hash} 表示敌手访问随机预言机 $O^{H_1}(\cdot)$ 的次数，而 t_{Hash} 表示 $H.Hash(\cdot)$ 的运行时间.

证明. 证明采用反证法. 对于签名方案 *SCH-2-DS*0，假设存在一个存在性伪造算法 $\mathcal{F}$，其运行时间为 t，其概率为 ε，敌手攻击签名方案的具体过程在定义 2 已经给出. 下面构造一个针对底层强变色龙 Hash 函数 *SCH* 的寻找碰撞算法，记作 C，其概率为 ε'，其运行时间约为 t'. 算法 C 模拟签名安全性定义中的挑战者，以子程序形式调用伪造算法 $\mathcal{F}$，最后给出一对碰撞.

首先，作为强变色龙 Hash 函数的攻击者，C 从它自己的挑战者处获得 Hash 密钥 hk，令签名公钥为 $pk=hk$，并把该公钥 pk 及其相关的辅助性公开参数发送给 $\mathcal{F}$. C 初始化一个计数器 $f=0$，用来跟踪记录在整个游戏期间各方访问随机预言机 $O^{H_1}(\cdot)$ 的次数，对重复消息的 Hash 函数值(随机预言机返回的值)只计一次.

C 按照如下方式模拟随机预言机 $O^{H_1}(\cdot)$. 对于

随机预言机询问 m,如果之前曾回答过该消息 m 的 Hash 值,则 C 只是简单地返回之前的 Hash 值;否则,C 随机选择 $s\in_R\hat{\mathcal{S}}$,计算 $(h,r)\leftarrow H.Hash(hk,s)$,取 $H_1(m)\leftarrow h=\mathrm{Hash}_{hk}(s,r)$,最后返回 $H_1(m)$作为应答. 上述模拟与随机预言机完全一致.

C 按照如下方式来模拟签名预言机. 不失一般性,我们假设所有提供给签名预言机 $O^{Sign}(\cdot)$ 的待签名消息各不相同. 为了模拟签名 $O^{Sign}(m)$,C 首先访问随机预言机 $O^{H_1}(\cdot)$,获得 Hash 值 $H_1(m)$,此处的随机预言机也是由 C 本身模拟. 根据上述对于随机预言机 $O^{H_1}(\cdot)$ 的模拟过程,存在 (s,r) 使得 $H_1(m)=\mathrm{Hash}_{hk}(s,r)$,而 (s,r) 正是由 C 本身选取. 因此,C 知晓 (s,r),可直接把消息 m 的签名定为 $\sigma\leftarrow(s,r)$,并将 σ 作为应答返回给伪造者 $\mathcal{F}$. 上述模拟与实际的签名算法完全一致.

最后,敌手 $\mathcal{F}$ 返回消息 m^* 及其伪造签名 σ^*. 如 $S.Vrf(pk,\sigma^*,m^*)\neq 1$,$C$ 则中断算法执行,宣布失败;如果 $S.Vrf(pk,\sigma^*,m^*)=1$,根据方案 *SCH-2-DS*0 中 $S.Vrf$ 的算法描述,可以知道 $h^*=\mathrm{Hash}_{hk}(s^*,r^*)$,此处 $\sigma^*=(s^*,r^*)$. 根据 $H_1(m^*)$的随机预言机模拟过程,C 知道另外一对碰撞值 $(s^{*\prime},r^{*\prime})$ 使得:

$$\mathrm{Hash}_{hk}(s^*,r^*)=\mathrm{Hash}_{hk}(s^{*\prime},r^{*\prime}).$$

C 把 $(s^{*\prime},r^{*\prime})$ 和 (s^*,r^*) 作为一对碰撞传给他本身的挑战者. 如此以来,只要 $(s^{*\prime},r^{*\prime})\neq(s^*,r^*)$,那么 C 就攻破了强变色龙 Hash 函数的抗碰撞性质.

现在分析事件 $(s^{*\prime},r^{*\prime})\neq(s^*,r^*)$ 发生的概率. 对于 C 在模拟过程中选定 (s^*,r^*),敌手仅知道对应的 Hash 值 $h=\mathrm{Hash}_{hk}(s^*,r^*)$. 在已知 Hash 值为 h 的条件下,$(s^{*\prime},r^{*\prime})$ 有 $|\hat{\mathcal{S}}|$ 种等概率的取值可能. 因此,伪造者输出的 (s^*,r^*) 等于 $(s^{*\prime},r^{*\prime})$ 的概率等于 $\frac{1}{|\hat{\mathcal{S}}|}$. 总之,只要伪造者 $\mathcal{F}$ 输出了合法签名且签名 $(s^{*\prime},r^{*\prime})\neq(s^*,r^*)$,则 C 就能够成功地输出一对碰撞. 因此,C 成功输出碰撞的概率为

$$\varepsilon'=Pr[C\ \text{succeeds}]=(1-\frac{1}{|\hat{\mathcal{S}}|})Pr[\mathcal{F}\ \text{succeeds}]=(1-\frac{1}{|\hat{\mathcal{S}}|})\varepsilon.$$

再来分析 C 的运行时间. C 的运行时间包括伪造算法 $\mathcal{F}$ 的运行时间和 C 模拟签名预言机和随机预言机的时间. 其中,一次签名预言机的模拟主要就是一次随机预言机的模拟,而随机预言机的一次模拟就是一次 Hash 函数 $\mathrm{Hash}_{hk}(s,r)$ 的计算,其运行时间记作 t_{Hash}. 同时,对于 C 中的一些琐碎的计算不予考虑,如某些结果的记录和查询. 因此,C 的运行时间为 $t'=t+q_{\mathrm{Hash}}\times t_{\mathrm{Hash}}$. 因此,所构造算法 C 是一个运行时间为 t'、成功概率为 ε' 的计算碰撞算法,这与变色龙 Hash 函数的 (t',ε') 抗碰撞性矛盾. 证毕.

4.2　不带状态的紧致安全签名方案

基于以上的带状态紧致安全签名方案 *SCH-2-DS*0,作如下修改可以得到一个不带状态的紧致安全签名方案,记作 *SCH-2-DS*1.

在密钥生成算法 $S.Gen(1^\lambda)$ 中,增加 $\mathcal{S}'$ 集合作为公共参数. 在下面定理中将会看到,该集合 $\mathcal{S}'$ 应该足够大,使得 $\frac{q_{\mathrm{sig}}^2}{|\hat{\mathcal{S}}||\mathcal{S}'|}$ 是一个可忽略的量.

在签名算法中,将操作 $h\leftarrow H_1(m)$ 改为

$$h\leftarrow H_1(m,s,s'),$$

此处 $s'\leftarrow_R\mathcal{S}'$. 其意义在于,通过参数 s' 在消息 m 的 Hash 值中增加足够大的随机因素.

在验证算法 $S.Vrf(pk,m,\sigma)$ 中,根据以上密钥生成算法和签名算法中的改动作相应的修改. 鉴于这些修改的平凡性,此处不作赘述.

定理 2. 如果底层的强变色龙 Hash 函数

$$SCH=(H.Gen,H.Hash,H.Ivt)$$

是 (t',ε') 抗碰撞的,那么上述签名方案

$$SCH\text{-}2\text{-}DS1=(S.Gen,S.Hash,S.Vrf)$$

就是 (t,ε) 存在性不可伪造的,其中:

$$\varepsilon'=(1-\frac{q_{\mathrm{sig}}^2}{|\hat{\mathcal{S}}||\mathcal{S}'|})(1-\frac{1}{|\mathcal{S}'|})\varepsilon,$$

$$t'=t+q_{\mathrm{Hash}}\times t_{\mathrm{Hash}},$$

其中,q_{Hash} 表示敌手访问随机预言机 $O^{H_1}(\cdot)$ 的次数,而 t_{Hash} 表示 $H.Hash(\cdot)$ 的运行时间.

证明. 与定理 1 的证明类似,此处从略. 证毕.

4.3　紧致安全签名方案实例

本节以基于 RSA 难题的强变色龙 Hash 函数为例,首先设计一个基于 RSA 的具体签名方案,然后考虑这一签名方案的变形,并比较这些方案与现有的相关方案. 借此说明,上述基于强变色龙 Hash 函数的一般化签名方案具有良好的理论概括性和实际应用价值.

对于前面提出的基于 RSA 假设的强变色龙 Hash 函数 *SCH-RSA*,应用上述的数字签名构造框架 *SCH-2-DS*0,得到带状态数字签名方案 *DS-RSA*:

1) $S.Gen(1^\lambda)$. 本方案相关符号与前面强变色龙 Hash 函数 *SCH-RSA* 一致,公钥和私钥分别为

$$pk=(n,e,x^e),$$
$$sk=(x,d),$$

子集合 $\hat{\mathcal{S}}\subset\{0,1,\cdots,e-1\}$ 满足条件 $|\hat{\mathcal{S}}|\geqslant 2$. 该集合与密码学意义下的 Hash 函数 $H_1:\{0,1\}^*\to\mathbb{Z}_n^*$ 作为公开参数全局公开.

2) $S.Sign(sk,m)$. 假设消息 m 之前未曾签过, 计算签名

$$\sigma=(H_1(m)^d\times x^{-s},s),$$

此处 $s\leftarrow_R\hat{\mathcal{S}}$.

3) $S.Vrf(pk,m,\sigma)$. 为了验证 $\sigma=(s,r)$ 是否为消息 m 的签名, 只需验证是否成立等式:

$$H_1(m)=(x^e)^s r^e \bmod n.$$

上述签名是直接套用签名框架 *SCH*-2-*DS*0 的结果, 因此具有带状态的缺点. 利用不带状态的签名框架 *SCH*-2-*DS*1, 并作适当优化, 可以构造出如下 2 个基于 RSA 假设的不带状态签名方案.

1) FDH 类签名方案. 在一般化的签名框架 *SCH*-2-*DS*1 中, 令 $\hat{\mathcal{S}}=\{0,1\}$, 则得形式签名:

$$\sigma=(H_1(m,s,s')^d\times x^{-s},s,s'),$$

此处 $s'\leftarrow_R\hat{\mathcal{S}}'$, $s\leftarrow_R\{0,1\}$. 与之相比, 著名的基于 RSA 的概率全域 Hash 签名 RSA-PFDH(probabilistic full domain Hash)[15-16] 则具有如下形式签名且也具有类似的紧致安全性:

$$\sigma=(H_1(m,s')^d,s'),$$
$$s'\leftarrow_R\mathcal{S}'.$$

由以上 2 式显然可见, 在计算上讲, 只是有一次模乘法的差别, 这与 d 次模幂运算相比, 基本可以忽略. 因此, 计算差别可以忽略. 在签名长度上看, 二者的签名长度只有 1 比特的差别, 考虑到紧致性方面的极细微差别, 1 比特的差别基本可以忽略.

2) Fiat-Shamir 类签名方案. 在一般化的签名框架 *SCH*-2-*DS*1 中, 令 $\hat{\mathcal{S}}=\mathbb{Z}_e$, $\mathcal{S}'=\varnothing$, 则得到形式的签名:

$$\sigma=(H_1(m,s)^d\times x^{-s},s),$$

此处 $s\leftarrow_R\mathbb{Z}_e$. 以上签名形式与文献[8]中基于 RSA 的紧致安全签名方案完全一致, 该方案是把文献[8]的一般化签名框架(称之为 SWAP 转换)应用在 GQ 身份认证方案[30] 而得到的. 注意: SWAP 提出的背景是为了解决 Fiat-Shamir 类签名方案的紧致安全性问题. 事实上, 一般的 Fiat-Shamir 类签名方案都不具有紧致安全性. SWAP 转换是 Fiat-Shamir 转换的一种变形, 仅适用于一类特殊的身份认证方案, 可以将其转化为紧致安全的 FS 类签名方案.

4.4 紧致安全签名构造框架的理论意义

通过 4.3 节具体例子, 对于本文提出的基于强变色龙 Hash 的一般化签名方案的构造框架, 作 4 项探讨:

1) 根据 4.3 节基于 RSA 难题的 3 个具体签名方案, 同样可以模块化地构造出基于双线性群上 CDH 难题的具体签名方案和基于整数分解难题的具体签名方案, 既包含 FDH 类紧致安全签名, 又包括 FS 类紧致安全签名.

2) 本文所提出的基于强变色龙 Hash 函数的紧致安全签名的框架, 在理论上统一了 FDH 类和 FS 类 这 2 类紧致安全签名方案, 从而指出了紧致安全签名方案要求底层密码原型所必须具有的最关键性质. 事实上, 在数字签名构造理论领域, 人们通常把 FS 类签名和 FDH 类签名看作 2 类独立的签名构造技术.

3) 在本文所提出的框架下, FS 类紧致安全签名[8] 和 PDH 类紧致安全签名, 可以看作是以不同方式调整框架中的相关参数而形成的不同的特殊结果. 特别是, FDH 类签名方案可以看作是比相应的 FS 类签名方案更为优化的形式. 从这层意义上讲, 本文的一般性理论结果粗略地否定了 FS 类紧致安全签名研究分支[3] 的研究意义.

4) 本文所提出的框架具有非常高的概括性, 从而具有广泛的应用性, 其根本原因是最为底层的密码原型具有很高抽象性和概括性. 事实上, 它可以诱导出陷门置换、无爪置换[15] 等非常基础的密码原型.

5 结 论

本文研究了可证明安全密码学领域的一个经典问题, 即如何由底层困难问题出发, 高效且直观地构造紧致安全数字签名方案. 首先扩展了传统变色龙 Hash 函数的概念, 提出了强变色龙 Hash 函数的密码原型, 用作底层困难问题的抽象模型, 力图刻划底层困难问题的基础密码性质, 而这些性质又是实现紧致安全签名的关键所在. 进而提出了一种直观、简练的转换框架, 可将强变色龙 Hash 函数转换为带状态的紧致安全签名方案. 进一步给出了对应的不带状态紧致安全签名方案变形, 并指出所提出的通用构造框架在某种程度上统一了 FS 类和 FDH 类 2 种经典的数字签名构造框架(就紧致安全签名的情况来说), 而之前密码学领域通常认为它们是互相

独立的 2 种签名构造范式.同时在本文所给的一般性框架下,FDH 类紧致签名还可以看作相应 FS 类紧致签名的优化变形.

参 考 文 献

[1] Feng Dengguo. Research on theory and approach of provable security[J]. Journal on Software, 16(10): 1743-1756 (in Chinese)
(冯登国. 可证明安全性理论与方法研究[J]. 软件学报, 2005, 16(10): 1743-1756)

[2] Xu Peng, Cui Guohua, Lei Fengyu. An efficient and provably secure IBE scheme without bilinear pairing [J]. Journal on Computer Research and Development, 2008, 45(10): 1687-1695 (in Chinese)
(徐鹏, 崔国华, 雷凤宇. 非双线性映射下一种实用的和可证明安全的 IBE 方案[J]. 计算机研究与发展, 2008, 45(10): 1687-1695)

[3] Chen Ming, Yuan Shaoliang. Provably secure identiy-based multi-proxy signature scheme in standard model[J]. Journal of Computer Research and Development, 2016, 53(8): 1879-1892 (in Chinese)
(陈明, 袁少良. 标准模型下可证明安全的基于身份多代理签名[J]. 计算机研究与发展, 2016, 53(8): 1879-1892)

[4] Wen Weiqiang, Wang Libin. A strongly secure lattice-based key exchange protocol [J]. Journal of Computer Research and Development, 2015, 52(10): 2258-2269 (in Chinese)
(温伟强, 王立斌. 基于格问题的强安全密钥交换协议[J]. 计算机研究与发展, 2015, 52(10): 2258-2269)

[5] Bellare M, Rogaway P. The exact security of digital signatures-how to sign with RSA and Rabin [G] //LNCS 1070: Advances in Cryptology (EUROCRYPT 1996). Berlin: Springer, 1996: 399-416

[6] Fiat A, Shamir A. How to prove yourself: Practical solutions to identification and signature problems [G] //LNCS 263: Advances in Cryptology (CRYPTO'86). Berlin: Springer, 1987: 186-194

[7] Goldwasser S, Micali S, Rivest R. A digital signature scheme secure against adaptive chosen-message attacks [J]. SIAM Journal on Computing, 1988, 17(2): 281-308

[8] Micali S, Reyzin L. Improving the exact security of digital signature schemes[J]. Journal of Cryptology, 1999, 15(1): 1-18

[9] Bellare M, Rogaway P. Random oracles are practical: A paradigm for designing efficient protocols[C] //Proc of ACM Conf on Computer & Communication Security. New York: ACM, 1993: 62-73

[10] Cramer R, Shoup V. Signature schemes based on the strong RSA assumption[J]. ACM Trans on Information & System Security, 1999, 3(3): 161-185

[11] Gennaro R, Halevi S, Rabin T. Secure Hash-and-sign signatures without the random oracle [G] //LNCS 1592: Advances in Cryptology (EUROCRYPT'99). Berlin: Springer, 1999: 123-139

[12] Hohenberger S, Waters B. Short and stateless signatures from the RSA assumption [G] //LNCS 5677: Advances in Cryptology (CRYPTO 2009). Berlin: Springer, 2009: 654-670

[13] Cash D, Hofheinz D, Kiltz E, et al. Bonsai trees, or how to delegate a lattice basis[J]. Journal of Cryptology, 2012, 25(4): 601-639

[14] Coron J S. On the exact security of full domain Hash[G] //LNCS 1880: Advances in Cryptology (CRYPTO 2000). Berlin: Springer, 2000: 229-235

[15] Dodis Y, Reyzin L. On the power of claw-free permutation [G] //LNCS 2576: Proc of the 3rd Int Conf on Security in Communication Networks. Berlin: Springer, 2002: 55-73

[16] Coron J S. Optimal security proofs for PSS and other signature schemes [G] //LNCS 2332: Advances in Cryptology (EUROCRYPT 2002). Berlin: Springer, 2002: 272-287

[17] Katz J, Wang Nan. Efficiency improvements for signature schemes with tight security reductions [C] //Proc of the 10th ACM Conf on Computer and Communications Security. New York: ACM, 2003: 155-164

[18] Boneh D, Lynn B, Shacham H. Short signatures from the weil pairing[J]. Journal of Cryptology, 2004, 17(4): 297-319

[19] Bellare M, Palacio A. GQ and schnorr identification schemes: Proofs of security against impersonation under active and concurrent attacks [G] //LNCS 2442: Advances in Cryptology (CRYPTO'02). Berlin: Springer, 2002: 162-177

[20] Pointcheval D, Stern J. Security arguments for digital signatures and blind signatures [J]. Journal of Cryptology, 2000,13(3): 361-396

[21] Schnorr C P. Efficient signature generation by smart cards [J]. Journal of Cryptology, 1991, 4(3): 161-174

[22] Abdalla M, Fouque P A, Lyubashevsky V, et al. Tightly-secure signatures from lossy identification schemes [J]. Journal of Cryptology, 2016, 29(3): 597-631

[23] Bellare M, Poettering B, Stebila D. From identification to signatures, tightly: A framework and generic transforms [G] //LNCS 10032: Advances in Cryptology (Asiacrypt 2016). Berlin: Springer, 2017: 435-464

[24] Goh E J, Jarecki S. A signature scheme as secure as the Diffie-Hellman problem [G] //LNCS 2656: Advances in Cryptology (EUROCRYPT 2003). Berlin: Springer, 2003: 401-415

[25] Goh E J, Jarecki S, Katz J, et al. Efficient signature schemes with tight reductions to the Diffie-Hellman problems [J]. Journal of Cryptology, 2007, 20(4): 493-514

[26] Krawczyk H, Rabin T. Chameleon signatures [C] //Proc of Network and Distributed System Security Symposium (NDSS 2000). Reston, VA: Internet Society, 2000: 143-154

[27] Chen Xiaofeng, Zhang Fangguo, Tian Haibo, et al. Discrete logarithm based chameleon hashing and signatures without key exposure [J]. Computers & Electrical Engineering, 2011, 37(4): 614-623

[28] Ateniese G, Medeiros B. On the key exposure problem in chameleon hashes [G] //LNCS 3352: Proc of Security in Communication Networks (SCN 2004). Berlin: Springer, 2004: 165-179

[29] Gao Wei, Wang Xueli, Xie Dongqing. Chameleon hashes without key exposure based on factoring [J]. Journal of Computer Science and Technology, 2007, 22(1): 109-113

[30] Quisquater J J, Guillou L C. A paradoxical identity-based signature scheme resulting from zero-knowledge [G] //LNCS 403: Advances in Cryptolgy (CRYPTO'88). Berlin: Springer, 1988: 216-231

Li Fei, born in 1977. PhD from Guangzhou University. Her main research interests include public key cryptography, algebra, and number theory.

Gao Wei, born in 1978. PhD from Hunan University. Associate professor. His main research interests include public key cryptography, cloud security and applied mathematics (mygaowei@163.cm).

Wang Guilin, born in 1968. PhD from Institute of Software, Chinese Academy of Sciences. Senior researcher. His main research interests include public key cryptography, cloud security and network security (Wang.Guilin@huawei.com).

Xie Dongqing, born in 1965. PhD from Hunan University. Professor. Member of CCF. His main research interests include applied cryptography, cloud security and network security (dongqing_xie@hotmail.com).

Tang Chunming, born in 1972. PhD. Professor. His main research interests include applied cryptography, cloud security and applied mathematics (ctang@gzhu.edu.cn).