哈希证明系统及应用研究

赵秀凤

(信息工程大学电子技术学院 郑州 450004)

摘 要 哈希证明系统在2002年欧密会上由Cramer和Shoup首次提出。哈希证明系统的概念自提出以来得到广泛研究,目前已有多个修改版本。"投影性"和"平滑性"是哈希证明系统的两个重要特性,正是由于这两个特性使得哈希证明系统除了用于设计CCA安全的公钥加密体制之外,还广泛应用于各种安全协议设计,比如:基于口令认证的密钥交换协议、不经意传输协议、可否认的认证协议、零知识证明协议和承诺协议等。介绍了哈希证明系统及其变形的各种定义,分析了定义之间的派生关系和安全级别关系,并讨论了哈希证明系统在密码学中的应用。

关键词 哈希证明系统,子集成员问题,CCA安全,密钥交换,OT协议,可否认认证,零知识证明,承诺协议

中图法分类号 TP309.2 **文献标识码** A

Research on Hash Proof System and its Applications

ZHAO Xiu-feng

(Institute of Electronic Technology, Information Engineering University, Zhengzhou 450004, China)

Abstract The notion of hash proof system was first proposed by Cramer and Shoup in Eurocrypt 2002. There are lots of research results about hash proof system since the notion was proposed, nowadays, some revisited versions were presented. "Projective" and "smoothness" are two important prosperities of hash proof system. It is found that hash proof system is used several contexts except used as a means to build efficient chosen-ciphertext secure public-key encryption schemes, such as password-based authenticated key exchange, oblivious transfer, deniable authentication, zero-knowledge proof, commitment, etc. We addressed the definitions of hash proof system, analyzed the derivation relations and security level among variations, and discussed the applications of hash proof system in cryptography.

Keywords Hash proof system, Subset member problem, CCA secure, Key exchange, OT protocol, Deniable authentication protocol, Zero-knowledge proof protocol, Commitment protocol

1 引言

Cramer和Shoup[1]首次定义了哈希证明系统(hash proof system, HPS)的概念。最初,哈希证明系统作为一类特殊的非交互证明系统,用于设计标准模型下可证明CCA2安全的公钥加密体制。哈希证明系统的概念自提出以来得到广泛研究,目前已有多个修改版本,例如:平滑投影哈希函数(smooth projective hash function, SPH)[2]、强 universal$_2$ 哈希证明系统[3]、可验证的Y-平滑投影哈希函数(verifiable Y-smooth projective hash function, V-Y-SPH)[4]。最近,Wee[5]提出了可抽取的哈希证明系统(extractable hash proof system, EHPS)。

哈希证明系统除了在公钥加密算法中的经典应用之外,还广泛应用于各种密码学协议的设计,如基于口令认证的密钥交换(password-based authenticated key exchange, PAKE)协议[2,6-10]、不经意传输(oblivious transfer, OT)协议[4,11-13]、可否认认证(deniable authentication, DA)协议[14-16]和零知识证明(zero knowledge proof, ZKP)协议[17]、承诺协议[18]等。

2 Cramer-Shoup定义

2002年,Cramer和Shoup提出了哈希证明系统的概念,并将其作为一个重要的密码学组件用于设计CCA2的公钥密码体制。哈希证明系统要求存在一个集合 X 和定义在 X 上的NP语言 L,使得区分 L 中的一个随机元素和 $X\backslash L$ 中的一个随机元素是计算困难的。哈希证明系统应用如此广泛,主要归功于哈希证明系统的两个完美特性,即"投影性"和"平滑性"。所谓"投影性",即哈希族中的每个哈希函数,对于 $x\in L$,有两种方式计算每个点的哈希函数值,它们分别是一个公开算法和一个秘密算法(分别对应投影密钥和哈希密钥)。所谓"平滑性",即给定投影密钥,对于 $x\in L$ 和 $x\in X\backslash L$ 两种情况下,哈希函数的输出是统计不可区分的。

2.1 通用投影哈希

令 X 和 Π 为有限非空集合,令 $H=(H_k)_{k\in K}$ 为由 K 标识的函数所组成的集合,对每个 $k\in K$,H_k 是从 X 到 Π 的一个函数。注意,对于 $k\neq k'$,允许 $H_k=H_{k'}$。我们称 $F=(H,K,X,\Pi)$ 为哈希族(hash family),其中每个 H_k 为一个哈希函数。

定义1(投影哈希族, projective hash family) 令 L 为 X

本文受国家自然科学基金(61173139)资助。

赵秀凤(1977—),女,博士生,讲师,主要研究方向为信息安全与密码学,E-mail:zhao_xiu_feng@163.com。

的非空子集，S 为有限非空的集合，令 $\alpha: K \to S$ 为函数。如果对所有的 $k \in K$，H_k 在集合 L 上的值由 $\alpha(k)$ 确定，称 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$ 为 (X,L) 的投影哈希族。通常，我们称 k 为哈希密钥，$\alpha: K \to S$ 为密钥投影函数，$s=\alpha(k)$ 为投影密钥。

定义 2（通用投影哈希族，universal projective hash family） 令 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$ 为投影哈希族，令 $\varepsilon \geqslant 0$ 为一个实数。考虑由 $k \in_R K$ 定义的概率分布：

称 $\boldsymbol{H}$ 是 ε-universal 的，如果对于所有的 $s \in S, x \in X \backslash L$，和 $\pi \in \Pi$，满足

$$\Pr[H_k(x)=\pi \wedge \alpha(k)=s] \leqslant \varepsilon \Pr[\alpha(k)=s]$$

称 $\boldsymbol{H}$ 是 ε-universal$_2$ 的，如果对于所有的 $s \in S, x \in X \backslash L$，$x^* \in X, x \neq x^*, \pi, \pi^* \in \Pi$，满足

$$\Pr[H_k(x)=\pi \wedge H_k(x^*)=\pi^* \wedge \alpha(k)=s] \leqslant \varepsilon \Pr[H_k(x^*)=\pi^* \wedge \alpha(k)=s]$$

如果 $\boldsymbol{H}$ 是 ε-universal 的，则已知 $\alpha(k)$ 的值，即使 H_k 由集合 L 完全确定，对于任意的 $x \in X \backslash L$，正确猜测 $H_k(x)$ 的概率至多为 ε。如果 $\boldsymbol{H}$ 是 ε-universal$_2$ 的，则除满足上述性质外，对于任意的 $x^* \in X \backslash L$，在 $\alpha(k)$ 和 $H_k(x^*)$ 固定的条件下，对于任意的 $x \in X \backslash L, x \neq x^*$，正确猜测 $H_k(x)$ 的概率至多为 ε。

这里需要说明的是 universality 是哈希证明系统的核心，它是证明 CCA2 安全性的关键所在。Universal 和 universal$_2$ 是一个安全性很强的概念，很多情况下很难有效实现 unvierisal 或 universal$_2$ 的投影哈希族，因此 Cramer 和 Shoup 给出了一个渐进性的概念，即平滑投影哈希族。

定义 3（平滑投影哈希族，smooth projective hash family） 令 $\boldsymbol{H}$ 是投影哈希族，按照如下方式定义两个随机变量 $U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$，随机选择 $k \in K$，随机选择 $x \in X \backslash L$，随机选择 $\pi' \in \Pi$，$U(\boldsymbol{H})=(x,\alpha(k),\pi')$，$V(\boldsymbol{H})=(x,\alpha(k),H_k(x))$。称 $\boldsymbol{H}$ 为 ε-平滑的，如果 $U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$ 是 ε-相邻的，即 $|U(\boldsymbol{H})-V(\boldsymbol{H})| \leqslant \varepsilon$。

2.2 子集成员问题

子集成员问题是平滑投影哈希函数的基础，在这里，我们给出子集成员问题的定义。符号说明：l 表示安全参数，$x \in_R S$ 表示从集合 S 中均匀选取元素 x，$\Lambda \leftarrow I$ 表示实例 Λ 选自 I 分布空间。

定义 4（子集成员问题，subset member problem） 假设分布空间 $(I_l)_{l \in N}$，对于每一个 l，I_l 是实例 Λ 的概率分布。子集成员问题 M 针对每一个实例 Λ 说明了 3 个有限非空集合 X,L 和 W，使得 L 是对应二元关系 $R \subset X \times W$ 的 X 的子集，即语言 $L=\{x: \exists w, s.t.(x,w) \in R\}$。

定义 5（可采样的子集成员问题，sample subset member problem） 称子集成员问题是可采样的，若满足下列条件：

(1)实例可采样：存在一个有效算法，输入 1^l，采样得到一个实例 $\Lambda=(X,L,W,R) \leftarrow I_l$。

(2)成员可采样：存在一个概率多项式算法，输入实例 $\Lambda=(X,L,W,R) \in M$，输出 $x \in L$ 和 $w \in W$ 使得 x 的分布是 L 统计可忽略的均匀分布。

(3)非成员可采样，存在概率多项式算法 $\mathcal{A}$，输入实例 $\Lambda=(X,L,W,R) \in M$ 和元素 $x_0 \in X$，输出 $x_1=\mathcal{A}(\Lambda,x_0)$，使得如果 $x_0 \in_R L$ 那么 x_1 的分布是 $X \backslash L$ 统计可忽略的均匀分布，如果 $x_0 \in_R X$ 那么 x_1 的分布是 X 统计可忽略的均匀分布。

定义 6（困难子集成员问题，hard subset member problem） 称 $M=(I_l)_{l \in N}$ 是困难子集成员问题，若两个分布空间 $\{\Lambda_l, x_l\}$ 和 $\{\Lambda_l, y_l\}$ 是不可区分的，其中 $\Lambda_l \leftarrow I_l$，$x_l \in_R L(\Lambda_l)$，$y_l \in_R X(\Lambda_l) \backslash L(\Lambda_l)$。

2.3 通用哈希证明系统

在上述困难子集成员问题的背景下，给出通用哈希证明系统的定义。

定义 7（哈希证明系统，hash proof system，HPS） 令 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$ 为 (X,L) 的投影哈希族，M 为子集成员问题，称满足下面条件的投影哈希族 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$ 为 M 的哈希证明系统 $\boldsymbol{P}$。

(1)对每个实例 $\Lambda \in M$，任意 $k \in K$，存在有效的算法用于计算 $\alpha(k) \in S$；

(2)给定 $k \in K$ 和 $x \in L$，可以有效计算 $H_k(x) \in \Pi$，这个算法称为 $\boldsymbol{P}$ 的秘密算法；

(3)给定 $\alpha(k)$，$x \in L$，及 x 的证据 w，存在有效算法 f 用以计算 $H_k(x)$，即 $f(x,\alpha(k))=H_k(x)$，称算法 f 为公开算法；

(4)存在有效的算法用于识别 Π 中的元素。

定义 8（通用哈希证明系统，universal hash proof system，UHPS） 令 $\varepsilon(l)$ 为一个函数，它将非负整数映射为非负实数。令 M 为子集成员问题，M 描述了所有实例分布的一个序列 $I(l)_{l \geqslant 0}$。令 $\boldsymbol{P}$ 为 M 的一个哈希证明系统，如果存在一个可忽略的函数 $\delta(l)$，使得对于所有的 $l \geqslant 0$，和所有的 $\Lambda[X,L,W,R] \in [I_l]$，针对实例 Λ，与哈希证明系统 $\boldsymbol{P}$ 关联的投影哈希族 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$ 与一个 $\varepsilon(l)$-universal(-universal$_2$, smooth) 的投影哈希族 $\boldsymbol{H}=(H,K,X^*,L^*,\Pi,S,\alpha^*)$ 是 $\delta(l)$-相邻的，则称 $\boldsymbol{P}$ 是 $\varepsilon(l)$-universal(-universal$_2$, smooth)。

3 修改的哈希证明系统

3.1 Gennar-Lindell 定义

在文献[1]中，平滑哈希证明系统作为一种特殊的非交换证明系统用于设计 CCA2 安全的公钥加密，而在文献[2]中，作者试图用 CCA2 安全的公钥加密体制构造这种完美性质的结构，并作为一个基本的组件设计安全高效的密钥协商协议。为了适应基于口令认证密钥协商的应用背景，Gennaro 和 Lindell 修改了 Cramer-Shoup 对哈希证明系统的原始定义，降低了“投影性”，加强了“平滑性”，并将“平滑的哈希证明系统”改称为“有效的平滑投影哈希函数”。

弱投影性 在 Cramer-Shoup 定义中投影函数对于集合 L 中的每个元素成立，即对于每个 $x \in L$ 都存在投影密钥函数 $\alpha: K \to S$ 使得投影密钥 $s=\alpha(k)$ 可以唯一确定 $H_k(x)$ 的值。而弱投影性的投影密钥函数是基于元素的，即输入哈希密钥 k 和一个元素 $x \in X$，输出投影密钥 $s_x=\alpha(k,x)$。若 $x \in L$，则给定 $s_x=\alpha(k,x)$ 唯一确定 $H_k(x)$。

强平滑性 在 Cramer-Shoup 定义中，平滑性要求 x 是在分布 $X \backslash L$ 中随机选择的，即 $x \in_R X \backslash L$。如果 x 是被敌手恶意选择的，则需要考虑关于每个 $x \in X \backslash L$ 投影哈希函数的平滑性。重新定义两个随机变量 $U(H)$ 和 $V(H)$，$U(H)=(x,\alpha(k),\pi')$，$V(H)=(x,\alpha(k),H_k(x))$，其中 $k \in_R K$，$\pi' \in_R \Pi$，x 是固定的。若对于每个 $x \in X \backslash L$，$U(H)$ 和 $V(H)$ 是统计不可区分的，即 $U(H) \overset{s}{\equiv} V(H)$，则称 $\boldsymbol{H}=(H_k,K,X,L,\Pi,\alpha,s)$ 是

平滑的。

3.2 Kurosawa-Desmedt 定义

Kurosawa 和 Desmedt[3] 在设计 IND-CCA 安全的混合加密体制时，修改了哈希投影哈希函数 Cramer-Shoup 定义，将其 ε-universal$_2$ 替换为强(strongly) universal$_2$.

定义 9(强通用投影哈希族，strongly universal projective hash family) 令 $\boldsymbol{H}=(H,K,X,L,\Pi,S,\alpha)$为投影哈希族，考虑由 $k\in_R K$ 定义的概率分布：

称 $\boldsymbol{H}$ 是强 universal 的，如果对于所有的 $s\in S, x\in X\backslash L$，和 $\pi\in\Pi$，满足

$$\Pr[H_k(x)=\pi|\alpha(k)=s]=\frac{1}{|\Pi|}$$

称 $\boldsymbol{H}$ 是强 universal$_2$ 的，如果对于所有的 $s\in S, x\in X\backslash L$，$x^*\in X, x\neq x^*$，$\pi,\pi^*\in\Pi$，满足

$$\Pr[H_k(x)=\pi|H_k(x^*)=\pi^*\wedge\alpha(k)=s]=\frac{1}{|\Pi|}$$

3.3 Kalai 定义

为了设计安全的 OT 协议，Kalai[4] 修改了 Gernaro-Lindell 的平滑投影哈希函数概念，提出了可验证的 Y-平滑投影哈希函数。其与 Cramer-Shoup 定义的平滑投影哈希函数的区别在于：第一，放松了平滑性要求，第二，增加了可验证性。

3.3.1 Y-平滑投影哈希函数

定义 10(Y-平滑投影哈希函数) 令 $\boldsymbol{H}=(H_k,K,X,L,\Pi,S,\alpha)$为困难子集问题 M 的投影哈希族，若对每个实例 $\Lambda=(X,L,W,R)$和每个 $x\in Y(\Lambda)$，其中 $Y\subseteq X\backslash L$，随机变量$(\alpha(k),H_k(x))$和$(\alpha(k),\pi)$是统计不可区分的，其中 $k\in_R K(\Lambda)$，$\pi\in_R\Pi(\Lambda)$，则称 $\boldsymbol{H}=(H_k,K,X,L,\Pi,S,\alpha)$是困难子集问题 M 的 Y-平滑投影哈希函数。

注意：Y-平滑投影哈希函数与 Cramer-Shoup 定义中的平滑投影哈希证明系统的区别有两点：第一，Y-平滑性适用于恶意选择的子集成员问题实例 Λ，而 Cramer-Shoup 定义中的平滑性仅适用于特定的 $\Lambda\in M$。第二，Y-平滑性要求对于每个 $x\in Y$ 成立，而 Cramer-Shoup 定义中的平滑性要求对于随机选择 $x\in_R X\backslash L$ 成立。

为什么要给出这样一个定义呢？原因在于当需要处理恶意选择实例 Λ 的情况时，令 $Y=X\backslash L$，然后构造$(X\backslash L)$-平滑投影哈希族。然而，我们不知道如何构造这样一个族，使得平滑性条件对于每个(甚至恶意选择的)实例 Λ 都成立。因此，文献[4]放松了平滑性要求，对于 $Y\subseteq X\backslash L$，仅要求 Y-平滑性。

3.3.2 可验证样本子集成员问题

定义 11(可验证样本子集成员问题) 称子集成员问题 M 是 Y-可验证样本，如果满足问题可采样、成员可采样和非成员可采样之外，还满足 Y-可验证，即：存在概率多项式算法 $\mathcal{B}$，输入是任意的三元组(Λ,x_0,x_1)，可验证存在比特 $b\in\{0,1\}$，使得 $x_b\in Y(\Lambda)$，即

(1)对于每个实例 Λ 和每个 x_0,x_1，若 $x_0\notin Y(\Lambda)$，且 $x_1\notin Y(\Lambda)$，则 $\mathcal{B}(\Lambda,x_0,x_1)=0$；

(2)存在 $b\in\{0,1\}$，若 $x_b\in L$，且 $x_{1-b}\in\mathcal{A}(\Lambda,x_b)$，那么 $\mathcal{B}(\Lambda,x_0,x_1)=1$。

3.4 Wee 定义

2010 年美密会上，Wee[5] 在 Cramer-Shoup 定义的基础上引入了可抽取的哈希证明系统的概念。可抽取的哈希证明系统也是一类特殊的非交互零知识证明系统，与 Cramer-Shoup 的通用哈希证明系统的区别在于用“知识证明”特性取代了“平滑性”。即，密钥可通过“模拟”和“抽取”两种方式生成。另外一个不同之处在于，Cramer-Shoup 定义的通用哈希证明系统依赖于困难子集成员问题，而 Wee 定义的可抽取的哈希证明系统依赖于困难查找问题。利用可抽取的哈希证明系统，我们可以全新的视角来设计 CCA-安全的公钥加密体制。

4 定义之间的关系

4.1 派生关系分析

这里我们给出哈希证明系统的各个定义之间的派生关系，如图 1 所示。其中“→”表示派生关系，“⇒”表示关联关系。

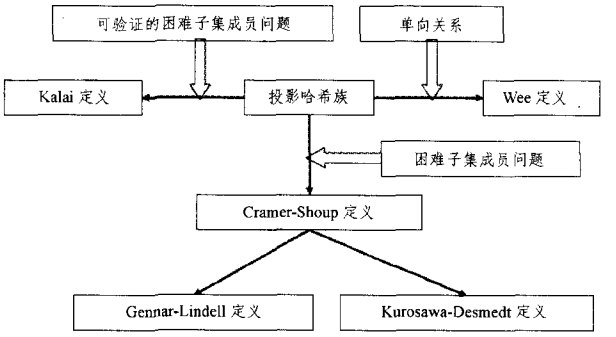

图 1 哈希证明系统定义之间的派生关系

4.2 安全级别分析

首先从定义 2 和定义 10 可直接得出 ε-universal$_2$⇒ε-universal 和 strongly universal$_2$⇒strongly universal。另外还有如下等价关系。

结论 1 $\frac{1}{|\Pi|}$-universal⇔strongly universal

证明：“⇒”假设 $\boldsymbol{H}$ 是 $\frac{1}{|\Pi|}$-universal 的，则对于所有的 $s\in S, x\in X\backslash L$ 和 $\pi\in\Pi$，对于随机选择的$k\in_R K$，下式成立

$$\Pr[H_k(x)=\pi\wedge\alpha(k)=s]\leqslant\frac{1}{|\Pi|}\Pr[\alpha(k)=s]$$

假设存在 $\hat{s}\in S, \hat{x}\in X$，和 $\hat{\pi}\in\Pi$ 使得对于随机选择的 $k\in_R K$，有

$$\Pr[H_k(\hat{x})=\hat{\pi}\wedge\alpha(k)=\hat{s}]<\frac{1}{|\Pi|}\Pr[\alpha(k)=\hat{s}]$$

那么，对于 $k\in_R K$，有

$$\begin{aligned}\Pr[\alpha(k)=\hat{s}]&=\sum_{\pi\in\Pi}Pr[H_k(\hat{x})=\pi\wedge\alpha(k)=\hat{s}]\\&=\sum_{\pi\in\Pi\backslash\{\hat{\pi}\}}\Pr[H_k(\hat{x})=\pi\wedge\alpha(k)=\hat{s}]+\\&\quad\Pr[H_k(\hat{x})=\hat{\pi}\wedge\alpha(k)=\hat{s}]\\&\leqslant\frac{|\Pi|-1}{|\Pi|}\Pr[\alpha(k)=\hat{s}]+\Pr[H_k(\hat{x})=\hat{\pi}\wedge\alpha\\&\quad(k)=\hat{s}]\\&<\frac{|\Pi|-1}{|\Pi|}\Pr[\alpha(k)=\hat{s}]+\Pr[\alpha(k)=\hat{s}]\\&=\Pr[\alpha(k)=\hat{s}]\end{aligned}$$

从而，得出矛盾，所以有

$$\Pr[H_k(x)=\pi\wedge\alpha(k)=s]=\frac{1}{|\Pi|}\Pr[\alpha(k)=s]$$

也即 $\Pr[H_k(x)=\pi|\alpha(k)=s]=\frac{1}{|\Pi|}$。根据定义 5，$\boldsymbol{H}$ 满足 strong universality。

"⇐"假设 $\boldsymbol{H}$ 满足 strong universality，则对于所有的 $s\in S, x\in X\backslash L$ 和 $\pi\in\Pi$，对于随机选择的 $k\in_R K$，下式成立：

$$\Pr[H_k(x)=\pi|\alpha(k)=s]=\frac{1}{|\Pi|}$$

也即 $\frac{\Pr[H_k(x)=\pi\wedge\alpha(k)=s]}{\Pr[\alpha(k)=s]}=\frac{1}{|\Pi|}$，根据概率知识有

$$\Pr[H_k(x)=\pi\wedge\alpha(k)=s]=\frac{1}{|\Pi|}\Pr[\alpha(k)=s]$$

$$\leqslant\frac{1}{|\Pi|}\Pr[\alpha(k)=s]$$

根据定义 2，$\boldsymbol{H}$ 满足 $\frac{1}{|\Pi|}$-universality。

同理可证明如下等价关系：

结论 2 $\frac{1}{|\Pi|}$-universal$_2\Leftrightarrow$strongly universal$_2$。

结论 3 smoothness(Gennar-Lindell 定义)⇒smoothness (Cramer-Shoup 定义)。

证明：假设投影哈希族 $\boldsymbol{H}$ 满足 Gernar-Lindell 定义的平滑性，则对于如下方式定义两个随机变量 $U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$，对于每个 $x\in X\backslash L$，随机选择 $k\in K$，随机选择 $\pi'\in\Pi$，$U(\boldsymbol{H})=(x,\alpha(k),\pi')$，$V(\boldsymbol{H})=(x,\alpha(k),H_k(x))$，$U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$ 是统计不可区分的。那么对于随机选取的 $x\in X\backslash L$，$U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$ 自然是统计不可区分的，因此 $\boldsymbol{H}$ 满足 Cramer-Shoup 定义的平滑性。

结论 4 $X\backslash L$-smoothness(Kalai 定义)⇒smoothness (Gennar-Lindell 定义)。

证明：假设投影哈希族 $\boldsymbol{H}$ 满足 Kalai 定义的 $X\backslash L$-平滑性，则对于每一个困难子集成员问题 M 的实例 Λ，令 $Y=X\backslash L$，满足 $Y\subseteq X\backslash L$，按照如下方式定义两个随机变量 $U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$，对于每个 $x\in Y$，随机选择 $k\in K$，随机选择 $\pi'\in\Pi$，$U(\boldsymbol{H})=(x,\alpha(k),\pi')$，$V(\boldsymbol{H})=(x,\alpha(k),H_k(x))$，$U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$ 是统计不可区分的。那么对于特定的一个困难子集成员问题 M 的实例 Λ'，对于每个 $x\in X\backslash L$，随机选择 $k\in K$，随机选择 $\pi'\in\Pi$，$U(\boldsymbol{H})=(x,\alpha(k),\pi')$，$V(\boldsymbol{H})=(x,\alpha(k),H_k(x))$，$U(\boldsymbol{H})$ 和 $V(\boldsymbol{H})$ 是统计不可区分的，因此 $\boldsymbol{H}$ 满足 Gennar-Lindell 定义的平滑性。

5 应用研究

本节描述哈希证明系统(平滑投影哈希函数)在公钥加密和各类密码协议中的应用。

5.1 CCA2 安全的公钥加密

1998 年，Cramer 和 Shoup[19] 基于 ElGaml 体制构造的 CS 体制是第一个在标准模型下 IND-CCA2 安全的高效加密方案，他们将方案的安全性规约为杂凑函数无碰撞和判断性 DH 问题，而不是某个简单的加密体制。

2002 年，Cramer 和 Shoup[1] 在 CS 体制的基础上做了推广，基于"哈希证明系统"获得了更加高效的 IND-CCA2 安全的 Crammer-Shoup 加密框架，其基本思想是利用哈希证明系统的"投影性"实现解密，利用"平滑性"完成安全性证明。Crammer-Shoup 框架及其各种变形的加密体制的安全性最终规约为判断性问题(如 DDH、DCR、DQR)。

随后，出现了许多利用"哈希证明系统"构造 CCA 安全的加密体制研究成果[3,20]。最近，2010 年美密会上，Wee[5] 通过可抽取的哈希证明系统给出了基于计算性问题的 CCA2 安全的公钥加密框架，其基本思想是利用"抽取模式"实现解密，利用"哈希模式(ABO 模式)"完成安全性证明。Wee 加密框架的安全性最终规约为查找问题(如整数分解、CDH)。

5.2 基于口令认证的密钥协商协议

基于口令的认证密钥协商协议允许用户仅凭一个较短的、易于记住的口令就可以生成高熵的会话密钥，避免了一般的认证密钥交换协议要求存在公钥基础设施或者是要求用户拥有存储长对称密钥的安全硬件等前提假设，极大地方便了用户使用并降低了系统实施成本，能够适应受限制的密码设备，有着较强的实用性。

2001 年，Katz 等人[21] 采用 CCA2 安全的 Cramer-Shoup 加密体制等密码学组件提出了第一个标准模型下可证安全的 PAKE 协议。协议中使用了平滑投影哈希函数的思想，但是，Katz 等人没有明确提出平滑投影哈希函数的概念。2002 年，Cramer 和 Shoup 提出了平滑投影哈希函数的概念。

2003 年，Gennaro 和 Lindell[2] 对 KOY 协议所用的密码学组件进行抽象，采用平滑投影 Hash 函数等抽象的密码学组件替代了 Cramer-Shoup 公钥加密体制，提出了标准模型下 PAKE 协议的一个一般框架，称为 GL 框架，使其可以被实例化成为基于 DDH 假设、二次剩余假设和 N 次剩余假设的不同具体协议。后来，在 KOY/GL 协议的基础上，利用平滑投影哈希函数为组件，出现了大量关于口令认证密钥协商的研究成果[6-10]。

KOY/GL 协议的基本思想：首先，协议的参与方共享公共参考串 ρ 及 CCA 安全的加密体制 ε。然后，协议参与方交换对共享口令的密文，再利用平滑投影哈希函数的特性，即有两种方式计算哈希函数的值，计算两对(密文/口令)平滑投影哈希函数值，其组合结果作为最终协商的会话密钥。为此，每个参与方随机选择一个哈希密钥，计算相应的投影密钥并发送给对方。

5.3 不经意传输协议

不经意传输协议(Oblivious Transfer Protocols，OTP)是密码学中的一个基本协议，可用于实现比特承诺，两方 Circuit Evaluation、安全多方计算、电子支付，网上交易等协议。在不经意传输协议初始阶段，发送者拥有两个信息 m_0 和 m_1，接收者 R 拥有一个选择比特 b；协议执行结束后，接收者 R 获得选择信息 m_b，但是不知道 m_{1-b} 信息，发送者不知道接收者 R 的选择比特 b。

2005 年，Kalai[3] 首次利用平滑投影哈希函数 $\boldsymbol{H}=(H_k, K, X, L, \Pi, \alpha, s)$ 给出了一个 OT 协议的通用框架。其基本思想是平滑投影哈希函数的"可投影性"实现 OT 协议的功能，利用"平滑性"保证接收者的安全，利用困难子集成员问题的"困难性"保证发送者的安全。

然而，该协议不能抵抗敌手恶意选择平滑投影函数。原因在于协议无法保证接收者选择 $x_{1-b}\in X\backslash L$，接收者可以选择 $x_0, x_1\in X$，从而可以同时获得两个消息 m_0 和 m_1。为了预防恶意的接收者同时获得两个信息 m_0 和 m_1，必须提供一种机制来保证 x_0 和 x_1 中至少有一个属于 $X\backslash L$。为此，Kalai 在困难子集成员问题的基础上，提出了 Y-可验证的困难子集问

题及相应的 Y-平滑投影哈希函数。

2006 年，冯涛等人[12]对 Y-SPH-OT 协议在 UC 框架下进行了分析，分析结果表明在静态半诚实攻击情况下 Y-SPH-OT 协议是 UC 安全的，在自适应攻击情况下不具有 UC 安全性。为了预防攻击者对密文消息传输的自适应攻击，文献[12,13]中分别使用了“NCE 体制”和“DTD 体制”来代替 Y-SPH-OT 协议中的明文消息，从而可以实现“明文消息的可仿真性”。

5.4 可否认的认证协议

在研究并行零知识证明协议时，Dwork 等[23]提出了并行可否认认证(concurrent deniable authentication，CDA)的概念。可否认认证协议是一个两方的通信协议，能够使接收者 R 确信认证者 T 想要对消息 m 认证，但是接收者 R 不能向第 3 方证明消息的来源；同时，消息 m 的认证者 T 也不能向第 3 方证明曾经向接收者 R 提供了认证的消息 m，该性质称为前向可否认性[16]。可否认性强化了安全协议的保密特性，并在互联网密钥交换协议、电子选举系统、电子商务系统等许多领域得到应用。

在认证协议中，消息认证者需要认证消息，为了绑定认证消息，可以通过零知识或者证人不可区分性来完成证明。冯涛等人使用可验证的平滑投影哈希函数(VSPH)，原因是 VSPH 具有证人不可区分性质，接收者(攻击者)实体区分 NP 问题的成员采样和非成员采样是可忽略的。

文献[14]利用可验证平滑投影哈希函数和非承诺加密体制，构造了一类新的并行可否认认证协议结构。文献[14]利用不经意传输的思想实现共享秘密信息获取。文献[15]基于陷门承诺构造了新的投影密钥函数，提出了可验证平滑投影散列函数，可否认认证方案仅仅需要使用 VSPH，从而提高了协议的计算效率和通信效率。

文献[16]利用投影哈希函数的完美性质构造了一个认证协议 $\hat{\lambda}_{Proj}$，其基本思想是：使用“投影性”完成认证性功能，使用“平滑性”完成安全性证明。

$\hat{\lambda}_{Proj}$ 协议对于诚实的验证者是可否认的，但是对于恶意的验证者需要增加一轮挑战应答子协议来证明可否认性。修改后的协议记为 $Den-\hat{\lambda}_{Proj}$，$Den-\hat{\lambda}_{Proj}$ 协议在顺序执行的情况下是可证明可否认的认证协议，在并发环境下，借助于时间假设模型，可以保证对数次执行的可证明可否认认证性。

5.5 零知识证明协议

零知识的概念最早由 Goldwasser 等人[24]提出，目前已成为构造安全协议的有效工具，尤其是在安全多方计算、认证协议、数字签名方面，人们利用零知识设计出了大量优良的算法。零知识证明协议是这样一些证明系统，它们可以使验证者确信断言的正确性，但同时不泄漏除了断言本身之外的任何知识。

文献[17]对“零知识”特性进行了弱化，提出了证据可排除的零知识概念。证据可排除的零知识证明协议使得证明者可以向验证者证明一个证据的知识，而且验证者可以确信断言的正确性和证据 w 的有效性，同时，证据 w 不属于被排除的证据集合，即 $(w,w')\notin Q$，其中 w' 由验证者选择。这个集合是由公开的关系 Q 和验证者的秘密输入决定的。

证据可排除的零知识协议可用于设计一类特殊的身份认证协议，比如验证者希望确信证明者的身份与当前被通缉的嫌疑犯的身份不匹配。保证匿名性的前提下，验证者能够确信证明者使用的证据与嫌疑犯的证据不相同，同时得不到证明者证据的任何信息。另外，协议不应该泄露关于嫌疑犯身份的任何信息。

文献[17]基于 Gennar-Lindell 定义的平滑投影哈希函数给出了证据可排除的零知识协议的通用构造，并在公共参考串模型中证明了协议的 UC 安全性。

5.6 承诺协议

承诺协议也是密码学中一个基本协议，可用于实现零知识证明和安全多方计算以及基于口令认证的密钥协商协议。承诺协议分为两个阶段：承诺阶段和解承诺阶段。承诺阶段允许用户对一个秘密值 x 承诺为公开值 C，解承诺阶段将承诺 C 打开为 x。承诺方案有两个基本的特性，即隐藏性(hiding)和绑定性(binding)。所谓隐藏性，是指承诺 C 不能泄露关于承诺值 x 的任何信息，所谓绑定性是指对 x 的承诺 C 只能打开为 x，不能打开为其他的值。

文献[18]定义了一种可抽取的承诺(extractable commitment)协议，所谓可抽取性是指存在一个有效的算法，称为抽取器(extractor)，它可以生成新的承诺参数(即，新的 CRS)，其分布和诚实产生的 CRS 分布是相同的，并且可以从任意承诺 C 中抽取承诺值 x。借助于平滑投影哈希函数(Gennar-Lindell 定义)，文献[18]构造了条件可抽取的承诺。

条件可抽取的承诺可用于公钥核证(certification of public key)，即保证加入系统的用户确实掌握相应的私钥。通常的方法是使用知识的零知识证明技术，如果存在一个有效的知识抽取器，则用户掌握相应的私钥。作者利用条件可抽取的承诺取代繁杂的知识证明，实现了公钥核证，由于证明中不需要“rewinding”技术，从而保证了并发性。

结束语 本文介绍了哈希证明系统及其变形的各种定义，并分析了定义之间的演化关系、安全级别关系及其应用背景。哈希证明系统具有良好的特性，可处理的密码算法和安全协议非常多，因此哈希证明系统有广泛的应用前景。本文的工作有助于理解哈希证明系统的本质思想，促进哈希证明系统的应用研究。

参 考 文 献

[1] Cramer R, Shoup V. Universal hash proofs and a paradigm for adaptive chosen ciphertext secure public-key encryption[C]// Proc. of Advances in Cryptology-Eurocrypt 2002, LNCS 2332. Berlin: Springer-Verlag, 2002: 45-64

[2] Gennaro R, Lindell Y. A framework for password-based authenticated key exchange[C]// Proc. of Advances in Cryptology-Eurocrypt 2003, LNCS 2656. Berlin: Springer-Verlag, 2003: 524-543

[3] Kurosawa K, Desmedt Y. A new paradigm of hybrid encryption scheme[C]// Proc. of Advances in Cryptology-CRYPTO 2004, LNCS 3152. Berlin: Springer-Verlag, 2004: 426-442

[4] Kalai Y. Smooth projective hashing and two-message oblivious transfer[C]// Proc. of Advances in Cryptology-Eurocrypt 2005, LNCS 3494. Berlin: Springer-Verlag, 2005: 78-95

[5] Wee H. Efficient chosen-ciphertext security via extractable hash proofs[C]// Proc. of Advances in Cryptology-Crypto 2010,

LNCS 6223. Berlin: Springer-Vedag, 2010: 314-332

[6] Canetti R, Halevi S, Katz J, et al. Universally composable password-based key exchange[C]// Proc. of Advances in Cryptology-Eurocrypt 2005, LNCS 3495. Berlin: Springer-Vedag, 2005: 404-421

[7] Abdalla M, Pointcheval D. A scalable password-based group key exchange protocol in the standard model[C]// Proc. of Advances in Cryptology-Asiacrypt 2006, LNCS 4284. Berlin: Springer-Verlag, 2006: 332-347

[8] Faster G R. shorter password-authenticated key exchange[C] // Proc. of TCC 2008, LNCS 4948. Berlin: Springer-Verlag, 2008: 586-606

[9] Groce A, Katz J. A new framework for password-based authenticated key exchange [EB/OL]. Cryptology ePrint Archive, Report 2010/147. http://eprint. iacr. org/ 2010 /147. pdf, 2010

[10] Katz J, Vaikuntanathan V. Round-optimal password-based authenticated key exchange [C] // Proc. of TCC 2011, LNCS 6597. Berlin: Springer-Verlag, 2011: 293-310

[11] 冯涛,马建峰. Y-SPH-OT 协议的安全性分析[J]. 计算机科学, 2006, 33(8): 125-129

[12] 李凤华,冯涛,马建峰. 基于 VSPH 的 UC 不经意传输协议[J]. 通信学报, 2007, 28(7): 28-34

[13] 冯涛,马建峰,李凤华. UC 安全的高效不经意传输协议[J]. 电子学报, 2008, 36(1): 17-23

[14] 冯涛,马建峰. 基于证人不可区分的通用可复合安全并行可否认认证[J]. 软件学报, 2007, 18(11): 2871-288

[15] 冯涛,李凤华,马建峰,等. UC 安全的并行可否认认证新方法[J]. 中国科学 E 辑:信息科学, 2008, 38(8): 1220-1233

[16] Raimondo M D, Gennaro R. New approaches for deniable authentication [J]. Journal of Cryptology, 2009, 22: 572-615

[17] Kiayias A, Zhou H-S. Zero-knowledge proofs with witness elimination[C]// Proc. of PKC 2009, LNCS 3494. Berlin: Springer-Verlag, 2009: 124-138

[18] Abdalla M, Chevalier C, Pointcheval D. Smooth projective hasing for conditionally extractable commitments [C]// Proc. of Advances in Cryptology-Crypto 2009, LNCS 5677. Berlin: Springer-Verlag, 2009: 671-689

[19] Cramer R, Shoup V. A practical public key cryptosystem provably secure against adaptive chosen ciphertext attack [C] // Proc. of Advances in Cryptology-CRYPTO 1998, LNCS 1462. Berlin: Springer-Verlag, 1998: 13-25

[20] Abe M, Gennaro R, Kurosawa K, et al. Tag-KEM/DEM: A new framework for hybrid encryption and a new analysis of Kurosawa-Desmedt KEM[C]// Proc. of Advances in Cryptology-EUROCRYPT 2005. LNCS 3494. Berlin: Springer-Verlag, 2005: 128-146

[21] Katz J, Ostrovsky R, Yung M. Practical password-authenticated key exchange provably secure under standard assumptions[C]// Proc. of Advances in Cryptology-Eurocrypt 2001, LNCS 2045. Berlin: Springer-Verlag, 2001: 475-494

[22] Dwork C, Naor M, Sahai A. Concurrent zero-knowledge [J]. J. ACM, Preliminary version in STOC'98, 2004, 51(6): 851-898

[23] Goldwasser S, Micali S, Rackoff C. The knowledge complexity of interactive proof systems [J]. SIAM Journal on Computing, 1989, 18(1): 186-208

(上接第 5 页)

[17] Shacham H, Page M, Pfaff B. On the Effectiveness of Address Space Randomization[C]// CCS '04 Proceedings of the 11th ACM conference on Computer and communications security, 2004. New York, NY, USA: ACM, 2004: 298-307

[18] Seacord R C. Secure Coding in C and C++. Addison-Wesley, 2006

[19] Dullien T, Kornau T, Weinmann R-P. A framework for automated architecture-independent gadget search[C]// Proceedings of the 4th USENIX Workshop on Offensive Technologies (WOOT), 2010. Washington, DC: USENIX Association, 2010

[20] Kornau T. Return Oriented Programming for the ARM Architecture [OL]. http://zynamics. com/downloads/kornau-tim—diplomarbeit—rop. pdf, Master thesis, Ruhr-University Bochum, Germany. 2009

[21] Davi L, mitrienkoy A, Sadeghi A-R, et al. Return-Oriented Programming without Returns on ARM [R]. Technical Report HGI-TR-2010-002, 2010. Ruhr University Bochum, Germany, 2010

[22] Checkowayy S, Daviz L, Dmitrienkoz A, et al. Return-Oriented Programming without Returns[C]// CCS'10 Proceedings of the 17th ACM conference on Computer and communications security, 2010. New York, NY, USA: ACM, 2010: 559-572

[23] Dullien T, Kornau T, Weinmann R-P. A framework for automated architecture-independent gadget search[C]// Proceedings of the 4th USENIX Workshop on Offensive Technologies (WOOT), 2010. Washington, DC: USENIX Association, 2010

[24] Chen Ping, Xing Xiao, Mao Bing. Automatic Construction of Jump-Oriented Programming Shellcode(on the x86)[C]// ASIACCS '11. HongKong, China, March 2011

[25] Onarlioglu K, Bilge L, Lanzi A, et al. G-Free: Defeating Return-oriented Programming through Gadget-less Binaries[C]// ACSAC'10. NY, USA, 2010

[26] Abadi M, Budiu M, Ligatti J. Control-Flow Integrity Principles, Implementations, and Applications [J]. ACM Transactions on Information and System Security (TISSEC), 2009, 1(4)

[27] Kiriansky V, Bruening D, Amarasinghe S. Secure Execution Via Program Shepherding[C]// the Proceedings of the 11th USENIX Security Symposium (Security '02), 2002. San Francisco, California, 2002: 191-206

[28] Daviy L, Sadeghiy A-R, Winandyz M. ROPdefender: A Detection Tool to Defend Against Return-oriented Programming Attacks [C]// ASIACCS '11 Proceedings of the 6th ACM Symposium on Information, Computer and Communications Security, 2011. New York, NY, USA ACM, 2011: 40-51

[29] Chen Ping, Xiao Hai, Shen Xiao-bin, et al. DROP: Detecting Return-oriented Programming Malicious Code[C]// Prakash A, Gupta I, eds. Fifth International Conference on Information Systems Security (ICISS 2010). volume 5905 of Lecture Notes in Computer Science, Springer, 2009: 163-177