诚实发送者承诺与诚实接收者承诺

黄桂芳* 胡 磊
(中国科学院研究生院信息安全国家重点实验室 北京 100049)

摘 要：诚实发送者承诺是为了构造非交互的非延展承诺而引入的。该文给出了两个诚实发送者承诺：第 1 个是诚实发送者统计绑定的，第 2 个是完全隐藏的。这两个协议都不是承诺方案。这说明诚实发送者承诺是弱于承诺方案的密码学原语。此外，该文定义了诚实接收者承诺，并给出了两个构造：第 1 个构造具有统计绑定性质，第 2 个构造具有诚实接收者完全隐藏性质。这两个方案都不是承诺方案，从而说明了诚实接收者承诺是弱于承诺方案的密码学原语。

关键词：密码学；承诺方案；诚实发送者承诺；诚实接收者承诺
中图分类号：TP309 **文献标识码**：A **文章编号**：1009-5896(2011)-04-0849-05
DOI: 10.3724/SP.J.1146.2010.00731

Honest-Sender Commitment and Honest-Receiver Commitment

Huang Gui-fang Hu Lei
(*State Key Laboratory of Information Security*, *Graduate University of Chinese Academy of Sciences*, *Beijing* 100049, *China*)

Abstract: Honest-sender commitments were introduced to construct non-interactive and non-malleable commitments. In this paper, two honest-sender commitments are given: The first one is honest-sender statistically binding and the second one is perfectly hiding. Neither of them is a commitment scheme, which implies that honest-sender commitment is a weaker cryptographic primitive than commitment scheme. In addition, this paper defines honest-receiver commitment and gives two constructions: The first one has the statistically binding property and the second has the honest-receiver perfectly hiding property. Both of them are not commitment scheme, which implies that honest-receiver commitment is a weaker cryptographic primitive than commitment scheme.

Key words: Cryptography; Commitment scheme; Honest-sender commitment; Honest-receiver commitment

1 引言

承诺方案是最基本的密码协议之一。它是一个高效的两方协议，由两个阶段组成：承诺阶段和揭开阶段。在承诺阶段，发送者对一个秘密值进行承诺并把承诺值发送给接收者。在这个阶段，要求任意概率多项式时间(Probabilistic Polynomial Time，简写为 PPT)的接收者都不能得到关于被承诺值的任何知识(隐藏性质)。在揭开阶段，发送者揭开其承诺，接收者检验这个揭开是否有效。在这个阶段，要求任意 PPT 的接收者不能把其承诺揭开成两个不同的值(绑定性质)。承诺方案已经被广泛应用于零知识证明[1−3]、安全多方计算[4]、签署电子合约[5]等各个方面。

根据绑定和隐藏性质的强弱，承诺方案分为以下几种：统计绑定承诺、完全绑定承诺、统计隐藏承诺和完全隐藏承诺。对于任意计算能力无界的发送者，若他把一个随机承诺值揭开成两个不同值的概率是可以忽略的(negligible)，则称该承诺方案是统计绑定的(statistically binding)。特别地，若任意计算能力无界的发送者只能把承诺值揭开成唯一的值，则称该承诺方案是完全绑定的(perfectly binding)。若对于不同消息的承诺是统计不可区分(或统计接近)的，则称该承诺方案是统计隐藏的(statistically hiding)。特别地，若对于不同消息的承诺是同分布的，则称该承诺方案是完全隐藏的(perfectly hiding)。

在一些实际应用中，承诺方案需要满足一些额外的性质。比如，在公平的合同竞标中，要求承诺方案具有非延展性质[6]。到目前为止，研究者们已经构造出很多非延展承诺方案[6−13]。其中，Damgard 等人[7]首次使用了诚实发送者承诺作为构造模块来构造非延展承诺方案。诚实发送者承诺是指满足隐

2010-07-12 收到，2010-12-13 改回
国家自然科学基金(60773134，61003276，60803128)，国家 863 计划项目(2006AA01Z416)，国家 973 计划项目(2007CB311201)和中国博士后基金(20100470598)资助课题
*通信作者：黄桂芳 gfhuang@gucas.ac.cn

藏性质和诚实发送者绑定性质的密码协议。在引入诚实发送者承诺的概念之前，很多非延展承诺方案都是使用普通的承诺方案作为子协议构造出来的[8−10]。而实际上，在证明非延展性质时，只需要子协议满足隐藏性质和诚实发送者绑定性质。因此，在构造非延展承诺方案时，可以使用诚实发送者承诺代替普通承诺方案作为子协议。

本文中，我们给出了两个诚实发送者承诺：第 1 个是诚实发送者统计绑定的，第 2 个是完全隐藏的。此外，本文定义了诚实接收者承诺，即：满足绑定性质和诚实接收者隐藏性质的密码协议。并且，构造了两个诚实接收者承诺：第 1 个是统计绑定的，第 2 个是诚实接收者完全隐藏的。然而，上述 4 个构造都不是承诺方案，这说明诚实发送者承诺和诚实接收者承诺都是弱于承诺方案的密码学原语。

文章组织如下：第 2 节给出了一些定义和记号。第 3 节给出了两个诚实发送者承诺。第 4 节定义了诚实接收者承诺并给出了两个构造。

2 预备知识

在这一节，介绍一些记号和定义。

若 A 是一个概率算法，则 $y \leftarrow A(x_1,x_2,\cdots)$ 表示如下实验：随机选取 r，$A(x_1,x_2,\cdots;r)$ 输出 y。若 S 是一个有限集，令 $\alpha \leftarrow S$ 表示从 S 中随机选取一个元素 α。

函数 $f(n)$ 称为是可忽略的，如果对于每个正多项式 $q(n)$，存在一个正整数 N，使得对于所有的 $n>N$，有 $f(n)<1/q(n)$。

承诺方案 承诺方案是由两个 PPT 机器 S 和 R 执行的两阶段的交互协议。K 是一个 PPT 的密钥生成器。输入 1^k，K 生成一个公开的 pk。每个 pk 对应着消息空间 M_{pk} 和承诺值空间 C_{pk}。在承诺阶段，对消息 $m \in M_{pk}$，发送者 S 通过与接收者 R 进行交互的方式产生承诺值 c，并把 c 发送给 R。在揭开阶段，S 把 c 对应的揭开消息 d 发送给 R，R 运行 PPT 算法 Dec 得到消息 m。若 $c \notin C_{pk}$ 或 d 不是 c 的有效揭开，$\mathrm{Dec}(pk,c,d)=\perp$。承诺方案需要满足以下两个性质：

(1)隐藏性质：对于任意 PPT 的接收者 R^*，对于随机产生的 pk (安全参数为 k)，对于两个不同的消息序列 $\{m_{pk}\}_{k\in N}$ 和 $\{m'_{pk}\}_{k\in N}$，它们对应的分布序列 $\{<S(m_{pk}),R^*>(pk)\}_{k\in N}$ 和 $\{<S(m'_{pk}),R^*>(pk)\}_{k\in N}$ 是计算不可区分的。其中 $<S(m),R^*>(pk)$ 表示在承诺 m 过程中 R^* 所得到的观察(view)。若这两个分布序列是统计不可区分的，称为统计隐藏性质。若这两个分布序列是同分布的，称为完全隐藏性质。

(2)绑定性质：对于任意 PPT 的发送者 S^*，有

$$\begin{aligned}&Pr[(m\neq m')\wedge(m,m'\neq\perp):pk\leftarrow K(1^k),\\&(c,d,d')\leftarrow<S^*,R>(pk),m=\mathrm{Dec}(pk,c,d),\\&m'=\mathrm{Dec}(pk,c,d')]\leq\mathrm{negl}(k)\end{aligned}\tag{1}$$

若式(1)对任意无限计算能力的 S^* 都成立，称为统计绑定性质。特别地，若对于无限计算能力的 S^*，式(1)中所描述的事件发生的概率是 0，称为完全绑定性质。

通常，把满足统计或完全绑定(隐藏)性质的承诺方案称为统计或完全绑定(隐藏)的承诺方案。

Naor 承诺方案[14] 设 $G:\{0,1\}^*\rightarrow\{0,1\}^*$ 是一个伪随机生成器，满足 $\forall s\in\{0,1\}^*$，$|G(s)|=3|s|$。

(1)承诺阶段：

(a)接收者随机选取 $r\in\{0,1\}^{3n}$ 并把 r 发送给发送者。

(b)接到 r 之后，发送者用如下方式对 $b\in\{0,1\}$ 进行承诺：随机选取 $s\in\{0,1\}^n$，若 $b=0$，他计算 $G(s)$ 并将其发送给 R；否则，他计算 $G(s)\oplus r$ 并将其发送给 R。

(2)揭开阶段：发送者把承诺阶段用到的 s 发送给 R。若 $G(s)=a$，R 输出 0；若 $G(s)\oplus r=a$，R 输出 1。其中 (r,a) 是 R 在承诺阶段所得到的观察。

Pedersen 承诺方案[15]：设 p,q 是两个随机产生的大素数且满足 $q\mid p-1$，$G\subseteq Z_p^*$ 是阶为 q 的群，g,h 是 G 的两个随机生成元。假设在群 G 上计算离散对数问题是困难的。为了对消息 $m\in Z_q$ 进行承诺，发送者随机选取 $r\in Z_q$ 并发送 $c=g^mh^r$ 给接收者。在揭开承诺 c 时，发送者把 (r,m) 发送给接收者。接收者运行 Dec 算法如下：检验 $c=g^mh^r$ 是否成立。若成立，Dec 输出 m；否则，Dec 输出 $\perp$。

定义 1(诚实发送者承诺[7]) 非交互诚实发送者承诺主要包括以下算法：K 是密钥生成算法，HSCom 是诚实发送者承诺算法，HSDec 是发送者的揭开算法。诚实发送者承诺需要满足以下两个性质：

(1)隐藏性质：对不同消息的承诺是计算不可区分的。

(2)诚实发送者绑定性质：对于任意 PPT 的发送者 $\mathcal{A}$，有

$$\begin{aligned}&Pr[pk\leftarrow K(1^k),m\leftarrow\mathcal{A}(pk),(c,d)\leftarrow\mathrm{HSCom}_{pk}(m),\\&d'\leftarrow\mathcal{A}(c,d),m'\leftarrow\mathrm{HSDec}_{pk}(c,d'):(m,m'\neq\perp)\\&\wedge(m'\neq m)]\leq\mathrm{negl}(k)\end{aligned}\tag{2}$$

若对于任意计算能力无界的发送者 $\mathcal{A}$，式(2)成立，称为诚实发送者统计绑定性质。

类似地，我们可以定义诚实发送者统计绑定的诚实发送者承诺和完全隐藏的诚实发送者承诺。前

者是指满足诚实发送者统计绑定性质的诚实发送者承诺，后者是指满足完全隐藏性质的诚实发送者承诺。

3　诚实发送者承诺

在这一节，我们构造了两个诚实发送者承诺。

3.1 诚实发送者统计绑定的诚实发送者承诺

设 $G:\{0,1\}^* \to \{0,1\}^*$ 是一个把 n 长比特串映射到 $3n$ 长比特串的伪随机生成器。

方案的构造：

(1) K: 输入 1^k， K 输出 1^n，其中 $n=\mathrm{poly}(k)$。

(2) HSCom：输入 1^n 和要承诺的值 $b\in\{0,1\}$，发送者随机选取两个比特串 $r\in\{0,1\}^{3n}, s\in\{0,1\}^n$，当 $b=0$ 时，发送 $G(s)$ 给接收者；否则，发送 $G(s)\oplus r$ 给接收者。

(3) HSDec: 设 c 是接收者在承诺阶段得到的观察。输入 c 和揭开消息 (r',s')，若 $c=G(s')$，则 HSDec 输出 0；若 $c=G(s')\oplus r'$，则 HSDec 输出 1；若 $c\neq G(s')$ 且 $c\neq G(s')\oplus r'$, HSDec 输出 $\perp$。

定理 1　上述“方案的构造”是具有诚实发送者统计绑定性质的诚实发送者承诺，但不是一个承诺方案。

证明　由伪随机生成器的伪随机性质可知，上面的构造是计算隐藏的。由 Naor 承诺方案的统计绑定性质可知，对于任意使用 HSCom 算法进行承诺的计算能力无界的发送者来说，只存在可忽略部分的承诺能够被揭开成两个不同的值。即：诚实发送者统计绑定性质成立。因此，上面的构造是具有诚实发送者统计绑定性质的诚实发送者承诺。

下面我们构造一个恶意的 PPT 发送者 S^*，使得 S^* 总是能够把他的承诺打开成两个不同的值。S^* 构造如下：S^* 首先计算 $r=G(s_1)\oplus G(s_2)$，其中 s_1 和 s_2 是随机选取的长度为 n 的比特串。然后，若 $b=0$，S^* 把承诺值 $c=G(s_1)$ 发送给接收者；若 $b=1$，他把承诺值 $c=G(s_2)$ 发送给接收者。在揭开阶段，S^* 把 (s_1,r) 发送给接收者。这样，S^* 能把承诺值 c 揭开成 0 和 1，即 S^* 打破了承诺方案的绑定性质。因此，上面的协议不是承诺方案。　　证毕

3.2 完全隐藏的诚实发送者承诺

方案的构造：

(1) K：$(p,q,g)\leftarrow K(1^k)$，其中参数 p,q,g 同 Pedersen 承诺方案中的定义。

(2) HSCom：为了对消息 $m\in Z_q$ 进行承诺，发送者首先随机选取 G 的一个生成元 h 和一个元素 $r\in Z_q$，然后他计算 $c=\mathrm{HSCom}((p,q,g),h,m)=g^m h^r$ 并把 c 发送给接收者。

(3) HSDec：设 c 是承诺阶段接收者得到的观察。在接到发送者的揭开消息 (h',m',r') 之后，若 $c=g^{m'}(h')^{r'}$，HSDec 输出 m'；否则，HSDec 输出 $\perp$。

定理 2　上述“方案的构造”是完全隐藏的诚实发送者承诺，但不是承诺方案。

证明　从 Pedersen 承诺方案可知，上面的方案中产生的承诺值在群 G 上是均匀分布的。因此，上面的协议是完全隐藏的。对于任意使用 HSCom 算法进行承诺的 PPT 的发送者来说，除了可忽略的概率之外，他不能把其承诺揭开成不同的值。所以，上面构造的协议是诚实发送者绑定的。因此，上面的方案是完全隐藏的诚实发送者承诺。

下面我们构造一个恶意的 PPT 的发送者 S^*，使得 S^* 能够打破承诺方案的绑定性质。S^* 构造如下：S^* 随机选取 $t\in Z_q$ 计算 $h=g^t$。为了对消息 m 进行承诺，S^* 计算承诺值 $c=g^m h^r=g^{m+tr}$。然后，通过计算 $r'=r+(m-m')t^{-1}\bmod q$，他能够把 c 揭开成任意消息 m'。因此，上面的构造不是承诺方案。　　证毕

4　诚实接收者承诺

在这一节，我们定义诚实接收者承诺并且给出两个诚实接收者承诺的构造。

定义 2(诚实接收者承诺)　诚实接收者承诺主要包含以下算法：S, HR 是两个 PPT 的交互机器，K 是能够输出一个公开值 pk 的承诺密钥生成器。在承诺阶段，对于输入 pk，S 通过和 HR 进行交互产生 m 的承诺值 c。在揭开阶段，S 把揭开消息发送给 HR，HR 运行算法 Dec 来验证这个揭开的有效性。

诚实接收者承诺需要满足以下两个性质：

(1) 诚实接收者隐藏性质：对于随机产生的 pk (相对于安全参数 k)，对于两个不同的消息序列 $\{m_{pk}\}_{k\in N}$ 和 $\{m'_{pk}\}_{k\in N}$，$\{<S(m_{pk}),HR>(pk)\}_{k\in N}$ 和 $\{<S(m'_{pk}),HR>(pk)\}_{k\in N}$ 是计算不可区分的。特别地，若这两个分布序列同分布，称之为诚实接收者完全隐藏性质。

(2)绑定性质：对于任意 PPT 的发送者 S^*，有

$$Pr[(m\neq m')\wedge(m,m'\neq\perp): pk\leftarrow K(1^k),(c,d,d') \leftarrow <S^*,HR>(pk), m=\mathrm{Dec}(pk,c,d), m'=\mathrm{Dec}(pk,c,d')]\leq \mathrm{negl}(k) \quad (3)$$

类似地，我们可以定义统计绑定的诚实接收者承诺和诚实接收者完全隐藏的诚实接收者承诺。前者是指具有统计绑定性质的诚实接收者承诺，后者是指具有诚实接收者完全隐藏性质的诚实接收者承诺。

4.1 统计绑定的诚实接收者承诺

设G_1,G_2是两个不同的伪随机生成器，输入n长比特串后，它们的输出都是$3n$长的比特串。

方案的构造：

(1) K：输入1^k，K输出1^n，其中$n=\mathrm{poly}(k)$。

(2)承诺阶段：

(a)接收者随机选取 3 个比特串$r_1,r_2\in\{0,1\}^{3n}$，$a\in\{0,1\}^n$并把r_1,r_2,a发送给发送者。

(b)在接收到消息r_1,r_2,a之后，要承诺消息$m=m_1\circ m_2\in\{0,1\}^2$，发送者均匀选取$s\in\{0,1\}^n$，若$a\neq 0^n$，他计算并发送$c=(c_1,c_2)=(\mathrm{Com}(m_1,r_1,G_1,s),\mathrm{Com}(m_2,r_2,G_2,s))$给接收者。否则，他计算并发送$c=(c_1,c_2)=(\mathrm{Com}(m_1,r_1,G_1,s),\mathrm{Com}(m_2,r_2,G_1,s))$给接收者。对于$i,j=1,2$，$\mathrm{Com}(m_i,r_i,G_j,s)$是使用伪随机生成器$G_j$的 Naor 承诺算法。

(3)揭开阶段：发送者把s发送给接收者。设$c=c_1\circ c_2$是接收者在承诺阶段得到的观察，接收者运行如下 Dec 算法来得到$m=m_1\circ m_2$：

(a)若$c_1=r_1\oplus G_1(s)$，则$m_1=1$。

(b)若$c_1=G_1(s)$，则$m_1=0$。

(c)若$c_2=G_2(s)$且$a\neq 0^n$，则$m_2=0$。

(d)若$c_2=r_2\oplus G_2(s)$且$a\neq 0^n$，则$m_2=1$。

(e)若$c_2=G_1(s)$且$a=0^n$，则$m_2=0$。

(f)若$c_2=r_2\oplus G_1(s)$且$a=0^n$，则$m_2=1$。

定理 3 上述“方案的构造”是一个具有统计绑定性质的诚实接收者承诺，但不是一个承诺方案。

证明 由 Naor 承诺方案的统计绑定性质可知，上面的协议具有统计绑定性质。当$a\neq 0^n$时，由伪随机生成器的伪随机性质可知，对于诚实的接收者来说，在承诺不同的消息时他所得到的观察是计算不可区分的。而诚实接收者选取$a=0^n$的概率是可忽略的，因此，上面的协议具有诚实接收者隐藏性质。从而，上面的构造是一个具有统计绑定性质的诚实接收者承诺。

下面我们构造一个 PPT 的恶意接收者R^*，使得R^*能够打破承诺方案的隐藏性质。R^*构造如下：在第 1 步中，R^*令$a=0^n$，然后他执行与诚实接收者相同的步骤。给定两个消息$v_1=10$，$v_2=01$和C_b，其中C_b是v_b的承诺值，$b\in\{1,2\}$是随机选取的，PPT 的区分算法D构造如下：设$C_b=C_{b1}\circ C_{b2}$，若$C_{b1}+C_{b2}=r_1$，则令$b=1$。若$C_{b1}+C_{b2}=r_2$，则令$b=2$。所以，D能够区分两个不同消息的承诺值。因此，上面构造的协议不是一个承诺方案。 证毕

4.2 诚实接收者完全隐藏的诚实接收者承诺

方案的构造：

(1) K：输入1^k，K输出(p,q,g)，其中参数p,q,g同 Pedersen 承诺方案中的定义。

(2)承诺阶段：

(a)接收者随机选取群G的两个生成元h_1,h_2，并把它们发送给发送者。

(b)在接收到h_1,h_2后，为了对消息$m\in Z_q$进行承诺，发送者随机选取$r\in Z_q$并计算$c_1=g^m h_1^r$，$c_2=g^m h_2^{-r}$，然后把$c=(c_1,c_2)$发送给接收者。

(3)揭开阶段：发送者发送(m,r)给接收者。设$c=(c_1,c_2)$是接收者在承诺阶段所得到的观察。Dec 算法运行如下：验证$c_i=g^m h_i^{(-r)^{i+1}}$是否成立，其中$i=1,2$。若以上两个验证均成立，Dec 输出m；否则，Dec 输出$\perp$。

定理 4 上述“方案的构造”是一个具有诚实接收者完全隐藏性质的诚实接收者承诺，但不是一个承诺方案。

证明 对于随机选取的生成元g,h_1,h_2，对于随机选取的$r\in Z_q$，$c_i=g_m h_i^{(-r)^{i+1}}$均匀分布在群G上。所以，诚实接收者完全隐藏性质成立。由 Pedersen 承诺的绑定性质可知，若 PPT 发送者能够把一个承诺值揭开成两个不同的值，则他能够计算出群G上的离散对数，这与我们的困难性假设矛盾。所以，上面的构造具有计算绑定性质。因此，上面的协议是一个具有诚实接收者完全隐藏性质的诚实接收者承诺。

下面我们构造一个 PPT 的恶意接收者R^*，使得R^*能够打破承诺方案的隐藏性质。R^*构造如下：在第一步，R^*选取$h=h_1=h_2$，然后他按照诚实接收者的步骤运行协议。给定两个不同的消息$m_1,m_2\in Z_q$和C_b，其中C_b是m_b的承诺值，$b\in\{1,2\}$是随机选取的，PPT 的区分算法D可以构造如下：设$C_b=(C_{b1},C_{b2})$，若$C_{b1}\cdot C_{b2}=g^{2m_1}$成立，$D$输出 1；若$C_{b1}\cdot C_{b2}=g^{2m_2}$成立，$D$输出 2。于是，$D$能够区分出对于不同消息的承诺。因此，上面的构造不是承诺方案。 证毕

5 结论

承诺方案是密码协议中最基本的密码协议之一。承诺方案需要满足两个性质：隐藏性质和绑定性质。若只满足隐藏(绑定)性质和诚实发送者(接收者)绑定(隐藏)性质，相应的密码协议就是诚实发送者(接收者)承诺。在本文中，通过构造具体的实例指出，诚实发送者承诺和诚实接收者承诺都是弱于承诺方案的密码学原语。

参 考 文 献

[1] Goldwasser S, Micali S, and Rackoff C. The knowledge complexity of interactive proof systems. *SIAM Journal on*

Computing, 1989, 18(1): 186–208.

[2] Goldreich O, Micali S, and Widerson A. Proofs that yields nothing but their validity or all languages in NP have zero knowledge proof systems. *Journal of ACM*, 1991, 38(3): 691–729.

[3] Goldreich O. Foundations of Cryptography-Basic Tools. Version 1, USA, Cambridge University of Press, 2001: 228–240.

[4] Goldreich O, Micali S, and Widerson A. How to play any mental game or a completeness theorem for protocols with honest majority. Proceeding of the 19th Annual ACM Symposium on Theory of Computing—STOC'87, New York, New York, USA, May 25–27, 1987: 218–229.

[5] Even S, Goldreich O, and Lempel A. A randomized protocol for signing contracts. *Communications of the ACM*, 1985, 28(6): 637–647.

[6] Dolev D, Dwork C, and Naor M. Non-malleable cryptography. *SIAM Journal on Computing*, 2000, 30(2): 391–437.

[7] Damgard I and Groth J. Non-interactive and reusable non-malleable commitment schemes. Proceedings of the 35th Annual ACM Symposium on Theory of Computing—STOC'03, San Diego, California, USA, June 9–11, 2003: 426–437.

[8] Di Crescenzo G, Ishai Y, and Ostrovsky R. Non-interactive and non-malleable commitments. Proceedings of the 30th Annual ACM Symposium on Theory of Computing—STOC'98, Dallas, Texas, USA, May 23–26, 1998: 141–150.

[9] Di Crescenzo G, Katz J, and Ostrovsky R, *et al.*. Efficient and non-interactive non-malleable commitments. In Advances in Cryptology—EUROCRYPT'01, Innsbruck, Tyrol, Australia, May 6–10, 2001, 2045: 40–59.

[10] Fischlin M and Fischlin R. Efficient non-malleable commitment schemes. In Advances in Cryptology—CRYPTO'00, Santa Barbara, California, USA, August 20–24, 2000, 1880: 413–431.

[11] Lin Hui-jia, Pass R, and Venkitasubramaniam M. Concurrent non-malleable commitments from any one-way function. Proceedings of the 5th Theory of Cryptography Conference—TCC'08, New york, USA, March 19–21, 2008, 4948: 571–588.

[12] Pass R and Rosen A. Concurrent non-malleable commitments. Proceedings of the 46th Annual IEEE Symposium on Foundations of Computer Science—FOCS'05, Pittsburgh, PA, October 22–25, 2005: 563–572.

[13] Zhang Zong-yang, Cao Zhen-fu, and Ding Ning, *et al.*. Non-malleable statistically-hiding commitment from any one-way function. In Advances in Cryptology—ASIACRYPT'09, Tokyo, Japan, December 6–10, 2009, 5912: 303–318.

[14] Naor M. Bit commitment using pseudo-randomness. *Journal of Crypto*, 1991, 4(2): 151–158.

[15] Pedersen T P. Non-interactive and information-theoretic secure verifiable secret sharing. In Advances in Cryptology—CRYPTO'91, Santa Barbara, California, USA, August 11–15, 1991, 576: 121–140.

黄桂芳：　女，1979 年生，博士后，研究方向为密码学理论.

胡　磊：　男，1967 年生，教授，博士生导师，主要从事密码学理论的研究.