高效的无证书的在线/离线签密方案

罗 铭 闻英友 赵 宏

(东北大学信息科学与工程学院 沈阳 110004)

摘 要 在线/离线签密方案具有资源耗费小的特点,但已有的在线/离线签密方案大多是是基于证书的密码体制或者基于身份的密码体制提出的,都存在证书的管理问题或密钥的托管问题。基于无证书密码体制的优点,提出了一种高效的无证书的在线/离线签密方案。分析表明,该方案不需要证书的管理,也没有密钥的托管问题,满足签密所要求的所有性质,且在效率上优于已有的基于身份的在线/离线签密方案以及无证书的签密方案。

关键词 在线/离线签密,无证书的密码系统,双线性对,随机预言模型

中图法分类号 TP393 **文献标识码** A

Efficient Certificateless On-line/Off-line Signcryption Scheme

LUO Ming WEN Ying-you ZHAO Hong

(School of Information Science and Engineering, Northeastern University, Shenyang 110004, China)

Abstract On-line/off-line signcryption has the characteristics of low computation cost. However, the existing on-line/off-line signcryption schemes are based on certificate public key cryp tography and identity-based cryptography, which have the problems of certificate management or key escrow. Based on the merit of certificateless public key cryptography, an efficient certificateless on-line/off-line signcryption was proposed. The result shows that the new on-line/off-line signcryption scheme solves all the problems of certificate management and key escrow, and also satisfies all the required characteristics of signcryption. It is more efficient than the existed ID-based on-line/off-line signcryption schemes and certificateless on-line/off-line signcryption schemes.

Keywords On-line/off-line signcryption, Certificateless cryptography, Bilinear pairings, Random oracle model

1 引言

使消息既保密又认证地传输是信息安全研究的主要目标之一。传统的方法是"先签名后加密",但该方法效率较低。为了提高效率,Zheng[1]于1997年提出了签密的概念,其基本思想是在同一个逻辑步骤内同时完成数字签名和加密两项功能。然而Zheng的方案中用户的公钥可以为任意的字符串,不具有真实性。传统的解决方法是利用公钥基础设施(PKI),即由可信中心通过证书把用户的身份和公钥绑定,但该方法面临证书管理复杂的问题。为了解决该问题,Shamir[2]提出了基于身份的公钥密码体制(ID-PKC),其中每个用户的公钥直接来自于自己的身份信息(如IP地址、电子邮件等),用户私钥由一个可信的私钥生成中心(PKG)生成。ID-PKC虽然避免了证书使用,但无法克服用户密钥托管问题,即PKG知道用户的私钥,因此可以伪造出用户的签密消息。2003年,Al-Riyami和Paterson[3]提出了无证书的公钥密码系统(Certificateless Public Key Cryptography, CL-PKC)的概念。在CL-PKC中,用户的验证与加密密钥包含一个用户的身份与一个用户自身产生的公钥,用户的私钥则是由用户以及一个被称作私钥生成中心KGC(Key Generation Centre)的可信第三方共同产生。CL-PKC的主要特点是不需要证书,并消除了ID-PKC中固有的密钥托管问题。Barbosa与Farshim[4]在2008年提出了无证书签密的概念以及相应安全模型的定义,并给出了一个有效的方案。随后,Wu与Chen[5]提出了目前需要对运算最少的无证书的签密方案。文献[6]提出了无证书的多接收者签密方案。

签密技术的良好特性,使其得到了广泛的应用,如电子现金支付、邮件认证和密钥分配等[7],构造出高效的签密方案成为了当今密码学的研究热点,目前更有效的签密方案是基于在线/离线签名,第一个在线/离线签名由Even, Goldreich和Micali提出[8],它的实现是将签名分成两个阶段,第一个是离线阶段:待签署的信息还未被确定,签名者做一些预处理工作;第二个阶段是在线阶段:一旦待签署的信息被确定,签名者利用预处理的结果,并使用非常短的时间完成签名。利用在线/离线签名构造的签密见文献[9,10],但文献[9]同样存在Zheng方案中无可信公/私钥对的缺陷,文献[10]也无法避免基于身份密码系统中固有的密钥托管问题。

本文结合无证书密码系统以及在线/离线签名的优点,提

到稿日期:2009-07-22 返修日期:2009-09-30 本文受国家自然科学基金资助项目(60602061),国家自然科学基金资助项目(60803131)资助。

罗 铭(1983—),男,博士生,主要研究方向为信息安全等,E-mail:luom@neusoft.com;闻英友(1974—),男,博士,主要研究方向为信息安全等;赵 宏(1954—),男,博士,教授,博士生导师,主要研究方向为信息安全等。

出了一种高效的无证书的在线/离线签密方案，并在随机预言模型中给出了安全性证明。在本方案中，计算量上只需要1次对运算，且当存在代理服务器时，客户端只需要一次点乘运算，而目前效率最高的无证书的签密方案需要2次对运算。因此，本方案更高效。

2 双线性对及相关困难假设

设 G_1 为素数 q 阶加法循环群，G_2 为同样阶的乘法循环群，$a,b\in Z_q^*$ 是两个随机数。

定义 1 称 G_1 和 G_2 之间的映射 $\hat{e}:G_1\times G_1\to G_2$ 为一个双线性对，该对满足如下性质：

(1) 双线性：对任意的 $P,Q\in G_1$，有 $\hat{e}(aP,bQ)=\hat{e}(P,Q)^{ab}$

(2) 非退化性：存在 $P,Q\in G_1$，使得 $\hat{e}(P,Q)\neq 1_{G_2}$

(3) 可计算性：存在一个有效算法计算 $\hat{e}(P,Q)$，其中 $P,Q\in G_1$

本文提出的无证书的在线/离线签密方案基于以下3个困难问题。到目前为止，这些问题都没有多项式时间的有效算法可以解决。

定义 2(椭圆曲线离散对数问题，Elliptic Curve DLP，EC-DLP) 给定一个群 G，定义其上的两点 $P,Q\in G$，寻找一整数 x，使在 G 中有 $xP=Q$。

定义 3(计算性 Diffie-Hellman，CDH 问题) 即给定〈P,aP,bP〉计算 abP。其中 $a,b\in Z_q^*$ 是两个随机数，$P\in G_1$。

定义 4(计算性双线性 DH，CBDH)问题 即给定〈P,aP,bP,cP〉计算 $\hat{e}(P,P)^{abc}$。其中 $a,b,c\in Z_q^*$ 是3个随机数，$P\in G_1$。

3 无证书的在线/离线签密方案

与大部分的签密方案[5,10]不同的是，我们设计的方案需要验证签名阶段发生在恢复消息阶段之前，即签名验证算法也可以交由 PS(Proxy Server)来执行，而同时 PS 不能解签密获得明文消息，从而在消息保密的基础上实现网络信息在传播路径上的认证，达到提高处理伪造签密消息的效率、减少用户终端的计算时间以及防范垃圾信息传播的目的。针对以上目标，本文设计了一种高效的无证书的在线/离线签密方案。本方案实现的具体细节如下。

KGC Setup：设 G_1 是由 p 生成的素数 q 阶加法循环群，G_2 是一个阶为 q 的循环乘法群，P 为 G_1 的1个生成元，1个双线性对映射 $\hat{e}:G_1\times G_1\to G_2$，3个安全的 Hash 函数 $H_1:\{0,1\}^n\times G_1\to G_1$，$H_2:(G_1)^4\times G_2\to\{0,1\}^n$ 与 $H_3:\{0,1\}^n\times(G_1)^4\to\{0,1\}^n$，KGC 随机选择一个随机数 $s\in Z_q^*$，计算 $P_{pub}=sP$。KGC 公开系统参数〈$G_1,G_2,\hat{e},q,P,P_{pub},H_1,H_2,H_3$〉，保密主密钥 s。

Generate-User-Keys(GUK)：输入 *params*，用户 U 选择一个随机数 $x_U\in Z_q^*$，计算 $PK_U=x_UP_{pub}$，则用户 U 的公钥为 PK_U，密钥值为 x_U，在这里设 A 的密钥值为 x_A，公钥为 $PK_A=x_AP_{pub}$；B 的公钥为 $PK_B=x_BP_{pub}$，密钥值为 x_B。

Extract-Partial-Private-Key(EPPK)：输入 *params*，KGC 主密钥 s，用户身份标识 ID_U 以及用户 U 的部分公钥 PK_U，计算 $Q_U=H_1(ID_U,PK_U)$，然后输出 $D_U=sQ_U$，定义发送者 A 的身份为 ID_A，部分私钥值为 $D_A=sQ_A=sH_1(ID_A,PK_A)$；接收者 B 的身份为 ID_B，部分私钥值为 $D_B=sQ_B=sH_1(ID_B,PK_B)$。

OffSign：在对消息进行签密之前，发送者 A 产生一个离线签名。首先 A 随机选择一个数 $k\in Z_q^*$，计算离线签名 $R=kP_{pub}$ 以及 $S=k^{-1}(D_A+(x_A)^{-1}Q_A)$，然后计算 $u=\hat{e}(D_A,Q_B)$ 以及会话密钥 $key=H_2(Q_A,Q_B,kPK_B,x_APK_B,u)$。

Signcrypt：发送者对消息进行在线签密。输入明文 m 以及离线签名(R,S)，计算密文 $y=key\oplus m$ 以及 $h=H_3(y,Q_A,Q_B,R,S)$，然后计算在线签名 $\sigma=khx_A$，最后输出签密消息 $SC=(\sigma,y,R,S)$。

AVerify：接收者或其代理服务器对签密消息(σ,y,R)进行验证。

1)计算哈希值 $h=H_3(y,Q_A,Q_B,R,S)$；

2)验证等式 $\hat{e}(S,\sigma P)=\hat{e}(Q_A,hPK_A+hP)$ 是否成立，若成立，则通过验证，否则输出 $\perp$。

Decrypt：接收者对密文 y 进行解密。输入签名消息 R 以及密文 y，计算 $u=\hat{e}(D_B,Q_A)$ 以及会话密钥 $key=H_2(Q_A,Q_B,x_BR,x_BPK_A,u)$，最后输出明文 $m=key\oplus y$。

4 安全性及效率分析

4.1 安全性

在安全概念中，定义两种任意多项式时间攻击者 $A_{i(i=1,2)}$，其中 A_1 不能获取 KGC 的主密钥，他可以产生一个新的公钥 PK_U^* 来替代用户 U 的公钥，但不能同时获取用户 U 的部分私钥 D_U；A_2 可以获取 KGC 的主密钥，但不能替换用户的公钥。

(1) 机密性

命题 1 在随机预言模型中，若存在一个敌手 A_1 能够在 t 时间内，以 ε 的优势获取明文(他最多能进行 q_i 次 H_i 询问$(i=1,2,3)$，q_k 次 GUK 询问，q_g 次 EPPK 询问，q_c 次 Corruption 询问，q_s 次 Signcrypt 询问，q_d 次 Unsigncrypt 询问)，则存在一个区分者 C，能够在 $o(t+(q_s+3q_d)T_e^{\wedge})$ 时间内，以 $Adv(C)>(\varepsilon-q_d/2^{k-1})*(1-2/q_g)/(q_1*(q_1-1))$ 的优势解决 CBDH 问题，其中 $T_e^{\wedge}$ 表示计算一次双线性对运算所需要的时间。

证明：假设区分者 C 接收一个随机的 CBDH 问题实例 (P,aP,bP,cP)，他的目标是计算出 $\hat{e}(P,P)^{abc}$。C 把 A_1 作为子程序并扮演 A_1 的挑战者。在挑战中，C 维护 $L_i(i=1,2,3)$，L_u，L_s，L_d 6张列表，这些列表开始都为空，$L_i(i=1,2,3)$ 分别用于跟踪 A_1 对预言机 $H_i(i=1,2,3)$的询问，L_u 用于模拟 GUK 预言机，L_s 用于模拟 Signcrypt 预言机，L_d 用于模拟 Unsigncrypt 预言机。挑战一开始，C 将系统参数发送给 A_1，其中 $P_{pub}=P_1=aP$(C 并不知道 a，它扮演 KGC 的主密钥)，然后 C 开始建立上述6张列表。

GUK 询问：对于用户 U 的 GUK 询问，C 首先从 Z_q^* 中随机选取 x_U，计算 $PK_U=x_UP_{pub}$，并将(ID_U,x_U,PK_U)添加到 L_u 中，回答 PK_U 给 A_1。

H_1 询问：C 首先从$\{1,2,\cdots,q_1\}$中选取两个随机数 i_a 与 i_b。假设 A_1 不会做重复的询问。对于 A_1 的第 i 次 H_1 询问，

如果 $i=i_a$，回答 $H_1(ID_U,PK_U)=P_2=bP$，设置 $ID_a=ID_U$ 并将$(ID_a,\perp,bP)$添加到 L_1 中；如果 $i=i_b$，回答 $H_1(ID_U,PK_U)=P_3=cP$，设置 $ID_b=ID_U$ 并将$(ID_b,\perp,cP)$添加到 L_1 中，否则从 Z_q^* 中随机选取 w，计算 $Q_U=wP$，并将(ID_U,w,Q_U)添加到 L_1 中，回答 $H_1(ID_U,PK_U)=Q_U$。

H_2 询问：如果$(Q_i,Q_j,kPK_j,x_iPK_j,u,h_2)$在表 L_2 中，返回 h_2；否则从 $\{0,1\}^n$ 中随机选取 h_2，将$(Q_i,Q_j,kPK_j,x_iPK_j,u,h_2)$添加到 L_2 中，返回 h_2。

H_3 询问：如果(y,Q_i,Q_j,R,S,h_3) 在表 L_3 中，返回 h_3；否则从$\{0,1\}^n$ 中随机选取 h_3，将(y,Q_i,Q_j,R,S,h_3)添加到 L_3 中，返回 h_3。

EPPK 询问：假设 A_1 在对执行 EPPK 询问前已经执行过 H_1 询问。如果 $ID_U\in\{ID_a,ID_b\}$，终止模拟；否则在表 L_1 中查找 ID_U对应的条目(ID_U,w)，计算 $D_U=wP_1$，返回 D_U。

Corruption 询问：假设 A_1 在对执行 Corruption 询问前已经执行过 GUK 询问。C 在表 L_u 中查找 ID_U 对应的条目(ID_U,x_U,PK_U)，返回 x_U。

Signcrypt 询问：敌手可以对明文 m、身份 ID_1 和 ID_2 执行 Signcrypt 询问，假设 A_1 在对 ID_1 和 ID_2 执行 Signcrypt 询问前已经执行过 GUK 询问。在此，分 3 种情况考虑。

(1) $ID_1\notin\{ID_a,ID_b\}$

C 首先对 ID_1 执行 EPPK 询问以及 Corruption 询问，然后运行 OffSign 算法来获得一个离线签名(R,S)，最后 C 执行 Signcrypt 算法获取签密消息 SC 并将结果 SC 发送给 A_1。

(2) $ID_1\in\{ID_a,ID_b\}$ and $ID_2\notin\{ID_a,ID_b\}$

C 首先对 ID_1 执行 Corruption 询问，对 ID_2 执行 EPPK 询问，然后 C 随机选择一个数 $k\in Z_q^*$，计算 $R=kP_{pub}$ 以及离线签名 $S=k^{-1}(PK_A+P)$，$u=\hat{e}(D_2,Q_1)$以及相应 key 值，接着 C 计算密文 $y=key\oplus m$ 和 $h=H_3(y,Q_1,Q_2,R,S)$，令 $\sigma=khb$(C 不能计算 σ，他只是认为 $\sigma=khb$)，最后输出签密消息 $SC=(\sigma,y,R,S)$，并将结果 SC 发送给 A_1。

(3) $ID_1,ID_2\in\{ID_a,{}_1D_b\}$且 $ID_1\neq ID_2$

C 首先对 ID_1 执行 Corruption 询问，然后 C 随机选择一个数 $k\in Z_q^*$，计算 $R=kP_{pub}$ 以及离线签名 $S=k^{-1}(PK_A+P)$，接着 C 随机选取 $u\in G_2$ 并计算相应 key 值，确定$(Q_1,Q_2,kPK_2,x_1PK_2,u,h_2)$是否属于 L_2，若属于则选择另一个随机数 u 重复上述过程来确认在 L_2 中不存在$(Q_1,Q_2,kPK_2,x_1PK_2,u,h_2)$，最后 C 计算密文 $y=key\oplus m$ 和 $h=H_3(y,Q_1,Q_2,R,S)$，令 $\sigma=khb$，并输出签密消息 $SC=(\sigma,y,R,S)$给 A_1。

Unsigncrypt 询问：假设 A_1 在对 ID_2 执行 Unsigncrypt 询问前已经执行过 GUK 询问。如果 $ID_2\in\{ID_a,ID_b\}$，C 返回“$\perp$”；否则 C 执行 AVerify 验证算法，如果签名无效，返回“$\perp$”，否则 C 对 ID_2 执行 EPPK 询问以及 Corruption 询问，最后执行 Decrypt 算法计算并返回 m 给 A_1。

在阶段 1 结束后，A_1 将输出两个希望挑战的身份$\{ID_A,ID_B\}(ID_A\neq ID_B)$和两个消息$\{m_0,m_1\}$。如果 $ID_A,ID_B\notin\{ID_a,ID_b\}$，$C$ 终止这个模拟；否则 C 随机选择一个数 $k\in Z_q^*$，计算 $R^*=kP_{pub}$ 以及离线签名 $S^*=k^{-1}(PK_A+P)$，$u^*=h$(h 就是 CBDH 问题的候选答案)，然后 C 计算相应 key 值，接着 C 计算密文 $y^*=key\oplus m$ 和 $h=H_3(y,Q_1,Q_2,R^*,S^*)$，令 $\sigma^*=khb$，最后 C 将挑战密文 $SC=(\sigma^*,y^*,R^*,S^*)$发送给 A_1。

A_1 经过第二轮的询问，这些询问同第一轮相同。在模拟结束时，A_1 输出一个 b'作为对 b 的猜测。如果 $b'=b$，C 输出 $h=u^*$ 作为 CBDH 问题的答案，否则 C 没有解决 CBDH 问题。

下面计算 C 成功的概率。如果 A_1 在第一阶段对 ID_a 或 ID_b 执行 EPPK 询问，C 将失败，由于 A_1 最多只能执行 q_k 次 EPPK 询问，因此 A_1 不对 ID_a 或 ID_b 执行 EPPK 询问的概率大于 $1-2/q_g$。对于 Unsigncrypt 询问，C 拒绝一个有效的签密消息的概率不会超过 $q_d/2^k$。第一阶段结束以后，由于 A_1 选择身份 ID_a 或 ID_b 进行挑战的概率为 $2/q_1$，因此 A_1 将以至少 $2/(q_1*(q_1-1))$的概率输出两个希望挑战的身份$\{ID_A,ID_B\}$。关于 C 的计算时间，每次 Signcrypt 询问最多需要 1 次双线性对运算，每次 Unsigncrypt 询问最多需要 3 次双线性对运算。因此，C 在 $o(t+(q_s+3q_d)T_{\hat{e}})$时间内解决 CBDH 问题的优势如下：

$$\begin{aligned}Adv(C)>&|P[b'=b|SC=\text{signcrypt}(m_b,R,S,ID_B,x_A)]-\\&P[b'=i|h\in G_2,i=0,1]|*(1-2/q_g)*2/(q_1*(q_1-1))\\=&|(\varepsilon+1)/2-q_d/2^k-1/2|*(1-2/q_g)*2/(q_1*(q_1-1))\\=&(\varepsilon-q_d/2^{k-1})*(1-2/q_g)/(q_1*(q_1-1))\end{aligned}$$

命题 2 在随机预言模型中，假设 CDH 问题是困难问题，本方案在敌手 A_2 进行适应性选择密文攻击下同样具有不可区分性。

(1)不可区分性

证明：假设任意多项式时间攻击者 A_2 获取了第 j 次会话产生的密文 $y_j=key_j\oplus m_j$，其中 $key_j=H_2(Q_A,Q_B,kPK_B,x_APK_B,u)$，进一步假设 A_2 获得发送者 A 以及接收者 B 的部分私钥 D_A 与 D_B。对于攻击者 A_2 来说，要想获得该次会话的明文 m_j 在计算上是不可行的，因为计算 key_j 还需要知道 kPK_B 或 x_BR，x_APK_B 或 x_BPK_A，这都将面临 CDH 数学难题。因此，本方案在敌手 A_2 进行适应性选择密文攻击下同样具有不可区分性。

(2)不可伪造性

证明：如果一个攻击者 $A_{i(i=1,2)}$ 试图伪造签密者 A 产生的签密消息 $SC=(\sigma=khx_A,y,R=kP_{pub},S=k^{-1}(D_A+(x_A)^{-1}Q_A)$，他需要通过 $PK_A=x_AP_{pub}$ 得到用户的部分私钥 x_A，这将面对离散对数问题，从而 A_i 伪造签密消息计算上是不可行的。因此本方案实现了签密消息的不可伪造性。

(3)不可否认性

证明：既然本方案是不可伪造的，如果签密者 A 确实签密过一个消息，他就不能够否认。

(4)公开验证性

证明：第 j 次方案发送者 A 对消息 m_j 生成签密消息 $SC=(\sigma,y,R,S)$后，只需提交(SC,ID_A,ID_B)给第三方验证者，验证者首先计算哈希值 $h=H_3(y,Q_A,Q_B,R,S)$，然后检验等式 $\hat{e}(S,\sigma P)=\hat{e}(Q_A,hPK_A+hP)$是否成立即可，从而达到可公开验证的目的。另外，由于第三方没有接收者 B 的私钥(D_B,x_B)而无法解密签密消息得到 m_j，因此本方案在保密性的基础上实现了公开验证性。

(5) 前向安全性

证明：假设任意多项式时间攻击者 $A_{i(i=1,2)}$ 获取了第 j 次会话密钥 $key_j = H_2(Q_A, Q_B, kPK_B, x_APK_B, u)$，进一步假设 A_i 获得发送者 A 的私钥 (D_A, x_A)，他要想获得第 i 次 $(i \neq j)$ 次会话密钥 $key_i = H_4(Q_A, Q_B, kPK_B, x_APK_B, u)$ 在计算上是不可行的，因为计算 key_i 需要知道 kPK_B 或 x_BR，这将面临 CDH 数学难题。因此，本方案满足前向安全性。

4.2 有效性

由于计算资源的限制，通信终端一直是签密方案效率的瓶颈，因此，以下从终端的角度出发来分析签密方案性能，包括计算量（不考虑离线计算量）与密文长度两方面，并与现有协议进行比较。如表 1 所列，第 2 列 $x+y+z$ 表示 x 次 G_2 中的指数运算次数，y 次 G_1 中的点乘运算次数以及 z 次双线性对运算次数，其中 (n) 表示可交于代理服务器执行的运算次数，$|G_1|$ 表示 G_1 中一个元素的长度，c 表示密文长度，k 表示一个 Z_q^* 上随机数的长度，h 表示一个 $\{0,1\}^n$ 上哈希值的长度。

从表 1 可以看出，本方案在计算量上是最优的。在密文长度方面，文献[4]较本方案少一个 Z_q^* 上随机数的长度，但该长度较 $|G_1|$ 与 c 的长度几乎可忽略不计。另外，当存在代理服务器时，本方案只需要一次点乘运算。由此可见，本方案更适合于网络安全应用。

表 1 有效性比较

方案	Cost	Len
方案[4]	1+5+(3)	$2\|G_1\|+c$
方案[5]	6+3+2	$2\|G_1\|+c+k+h$
方案[10]	0+4+3	$2\|G_1\|+c+k$
新方案	0+[1+(2)]+(1)	$2\|G_1\|+c+k$

结束语 本文结合无证书密码系统与在线/离线签名的优点，提出了一个高效的无证书的在线/离线签密方案，并在随机预言模型中给出了安全性证明。在 CBDH 与 CDH 问题是困难的假设下，本方案被证明是安全的，而且利用无证书密码系统还避免了基于 PKI 密码体系证书管理复杂性以及基于身份密码系统固有的密钥托管问题。与现有的签密方案相比，本方案效率更高，且当存在代理服务器时，只需要一次点乘运算。将来的工作是设计通用的以及更为有效的无证书的在线/离线签密方案。

参 考 文 献

[1] Zheng Y. Digital signcryption or how to achieve cost (signature & encryption) (cost (signature) + cost (encryption)) [C] // Proceedings of the Cryptology-CRYPTO'97. Santa Barbara, California, USA, 1997: 165-179

[2] Shamir A. Identity-based cryptosystems and signature schemes [C] // Proceedings of the Cryptology - CRYPTO'84. Santa Barbara, California, USA, 1984: 47-53

[3] Al-Riyami S S, Paterson K G. Certificateless Public Key Cryptography [C] // Proceedings of the ASIACRYPT 2003. Taipei, Taiwan, 2003: 452-473

[4] Barbosa M, Farshim P. Certificateless Signcryption [EB/OL]. http://eprint.iacr.org/2008/143.pdf, 2008

[5] Wu Chen-huang, Chen Zhi-xiong. A New Efficient Certificateless Signcryption Scheme [C] // Proceedings of the ISISE'08. Shanghai, China, 2008: 661-664

[6] Selvi S S D, Vivek S S, Shukla D, et al. Efficient and Provably Secure Certificateless Multi-receiver Signcryption [C] // Proceedings of the ProvSec 2008. Shanghai, China, 2008: 52-67

[7] 李发根，胡予濮，李刚. 一个高效的基于身份的签密方案 [J]. 计算机学报，2006，29(9)：1641-1647

[8] Even S, Goldreich O, Macali S. On-line/off-line digital signatures [J]. Journal of Cryptology, 1996, 9: 35-67

[9] Zhang F, Mu Y, Susilo W. Reducing security overhead for mobile networks [C] // Proceedings of the 19th International Conference on Advanced Information Networking and Applications. Taipei, Taiwan, 2005: 398-403

[10] Sun Dong-dong, Huang Xin-yi, Mu Yi, et al. Identity-Based On-line/Off-line Signcryption [C] // Proceedings of the IFIP International Conference on Network and Parallel Computing. Shanghai, China, 2008: 34-41

(上接第 83 页)

参 考 文 献

[1] Wang Yao, Wenger S, Wen Jiantao, et al. Error resilient video coding techniques[J]. IEEE Signal Processing Magazine: 2000, 17(4): 61-82

[2] Wang Yao, Zhu Qinfan. Error control and concealment for video communication: a review[J]. Proceedings of the IEEE, 1998, 86(5): 974-997

[3] He Zhihai, Cai Jianfei, Chen Changwen. Joint source channel rate-distortion analysis for adaptive mode selection and rate control in wireless video coding[J]. IEEE Transactions on CSVT, 2002, 12(6): 511-523

[4] Ru Congchong, Yin Liuguo, Lu Jianhua, et al. UEP Video Transmission Based on Dynamic Resource Allocation in MIMO OFDM System[C] // Proceedings, 2007 IEEE Wireless Communications and Networking Conference (WCNC'07). 2007: 310-315

[5] Wang Yu, Chau Lap-Pui, Yap Kim-Hui. A Novel Resynchronization Method for Scalable Video Over Wireless Channel[C] // 2006 IEEE International Conference on Multimedia and Expo. 2006: 1669-1672

[6] Fang Tao, Chau Lap-Pui. Efficient content-based resynchronization approach for wireless video[J]. IEEE Transactions on Multimedia, 2005, 6(7): 1021-1027

[7] ITU-T. Video coding for low bit rate communications[S]. ITU-T Recommendation H.263, 1998

[8] MPEG-4 Video Verification Model version 18.0[S]. ISO/IEC JTC1/SC29/WG11 N3908 January 2001/Pisa

[9] Stuhlmuller K, Farber N, Link M, et al. Analysis of video transmission over lossy channels[J]. IEEE Journal on Selected Areas in Communications, 2000, 18(6): 1012-1032

[10] Stockhammer T, Hannuksela M M, Wiegand T. H.264/AVC in Wireless Environments[J]. IEEE Transactions on Circuits and Systems for Video Technology, 2003, 13(7), 657-673