第35卷 第15期 计 算 机 工 程 2009年8月
Vol.35 No.15 Computer Engineering August 2009
·安全技术· 文章编号：1000—3428(2009)15—0151—02 文献标识码：A 中图分类号：TP309.2

多接收者基于身份签密方案的密码分析

孙 迅[1]，李建华[1,2]，陈恭亮[2]，柳 宁[1]
(1. 上海交通大学电子工程系，上海 200240；2. 上海交通大学信息安全工程学院，上海 200240)

摘 要：针对一个多接收者基于身份签密方案，从签密方案的安全属性入手，分析其安全性。通过2个成功的攻击证明该方案不满足语义安全性和不可伪造性要求，存在对任何消息和任何身份伪造密文的有效算法。提出一个改进的多接收者基于身份签密方案并给出安全性证明。

关键词：基于身份签密；多接收者；语义安全；不可伪造性

Cryptanalysis of Identity-based Signcryption Scheme for Multi-receiver

SUN Xun[1], LI Jian-hua[1,2], CHEN Gong-liang[2], LIU Ning[1]
(1. Department of Electronic Engineering, Shanghai Jiaotong University, Shanghai 200240;
2. School of Information Security Engineering, Shanghai Jiaotong University, Shanghai 200240)

【Abstract】 Aiming at an identity-based signcryption scheme for multi-receiver beginning with the security attribute, this paper studies the security property of this scheme. It is proved that this scheme is neither semantically secure nor unforgeable with two successful attacks. There effective algorithms for forgery of any message or identity. An improved identity-based signcryption scheme for multi-receiver is proposed with security proof.

【Key words】 identity-based signcryption; multi-receiver; semantic security; unforgeability

1 概述

文献[1]提出数字签密(digital signcryption)[0]的概念，目的是以较高的效率同时完成签名和加密。签密的安全性属性[2]包括作为加密方案的语义安全性(semantic security)和作为签名方案的存在不可伪造性(existential unforgeability)。文献[3]首次提出基于身份签密(Identity-based Signcryption, IBSC)的概念，并设计了一个具体方案。其后，研究者相继提出了一些基于身份的签密方案[4-7]。

文献[8]提出多接收者基于身份签密(multi-receiver IBSC)的概念，在其模型中，发送者通过一次操作将一条消息的密文同时发送给多个接收者。文献[8]构造了一个基于双线性配对的具体方案，并证明其安全性。为了将一个消息发送给n个接收者，该方案在签密阶段只要执行一次配对操作。文献[9]提出另一个多接收者IBSC方案，并进行安全性证明。该方案比文献[8]方案更高效。在解签密阶段，文献[8]方案需要执行4次配对操作，文献[9]方案只需3次。

本文指出文献[9]方案不满足基于身份签密的安全性要求，即不满足语义安全性并且是通用可伪造的(universally unforgeable)。因此，与存在伪造相比，通用伪造对方案安全性的危害更大。

2 多接收者基于身份签密方案

一个多接收者基于身份签密方案可以描述为一个4元组(系统建立算法 Setup，私钥提取算法 Keygen，签密算法 Signcrypt，解签密算法 Designcrypt)。基于文献[10]基于身份的签密方案，文献[9]方案的工作方式如下：

(1)Setup。给定安全参数 k，私钥生成器(PKG)选择阶同为素数 q 的循环加法群 G_1 和乘法群 G_2，G_1 的生成元 P，一个双线性映射 e: $G_1 \times G_1 \rightarrow G_2$ 和3个哈希函数 H_0: $\{0,1\}^* \rightarrow G_1$，$H_1$: $G_1 \times \{0,1\}^* \rightarrow \square_q^*$ 和 H_2: $G_2 \rightarrow \{0,1\}^l$，其中，$l$ 是待签密消息的比特长度。PKG 选取主密钥 $s \in Z_q^*$ 和随机元素 $R \in G_1^*$，计算 $P_{pub}=sP$ 和 $\theta=e(R, P_{pub})$。PKG 公开系统参数 $(G_1,G_2,P,P_{pub}, R,\theta,e,H_0,H_1,H_2)$ 并秘密保管 s。

(2)Keygen。给定用户身份 ID_U，PKG 计算公钥 $Q_U=H_0(ID_U)$ 和对应的私钥 $D_U=sQ_U$。

(3)Signcrypt。为了发送消息 m 给 n 个接收者 $ID_1, ID_2,\cdots,ID_n$，身份为 ID_A 的发送者 Alice 执行如下操作：

1)选择 $r \in \square_q^*$，计算 $X=rQ_A$, $h_1=H_1(X,m)$ 和 $Z=(r+h_1)D_A$。

2)计算 $U=rP$, $\omega=e(Z,P)$, $c=m \oplus H_2(\omega)$ 和 $W=\theta^r\omega$。对于 $i=1, 2,\cdots,n$，计算 $T_i=rH_1(ID_i)+rR$。

之后，Alice 设定密文为 $\sigma=(c, U, X, W, T_1,\cdots,T_n, \Lambda)$，其中，$\Lambda$是一个标签，用来描述 T_i 与 ID_i 的关联。

(4)Designcrypt。从 Alice 收到密文 σ 后，每个接收者 ID_i 执行如下操作：

1)计算 $\omega'=W \cdot e(U,D_i) \cdot e(P_{pub},T_i)^{-1}$ 和 $m'=c \oplus H_2(\omega')$。

2)计算 $Q_A=H_0(ID_A)$ 和 $h_1'=H_1(X,m')$。

3)验证等式 $\omega'=e(P_{pub},X+h_1'Q_A)$。如果等式成立，则输出

基金项目：国家“863”计划基金资助项目“信息安全增值服务平台(东部)”(2005AA145110)；浦东新区科技创新公共服务平台基金资助项目(PDPT2005-04)

作者简介：孙 迅(1981－)，男，博士研究生，主研方向：信息安全；李建华、陈恭亮，教授、博士生导师；柳 宁，博士

收稿日期：2009-02-26 **E-mail：**xun.sun.cn@gmail.com

消息 m'，并认定 σ 有效。否则输出特殊字符⊥，表示 σ 不是有效的密文。

3 文献[9]方案的密码分析

从语义安全性和不可伪造性 2 个方面指出文献[9]方案不具有安全性。

3.1 对语义安全性的攻击

签密方案的语义安全性要求攻击者不能以不可忽略的优势区分一个有效密文 σ 是对消息 m_0 和 m_1 中哪个签密得到的。

假设 $\sigma=(c, U, X, W, T_1,\cdots, T_n, \Lambda)$是发送者 Alice 对 m_0 和 m_1 中的一个生成的有效密文。攻击者A以如下方式验证 σ 是否是由 Alice 对 m_0 生成的密文，从而破坏方案的语义安全性：

(1)计算 $h_1'=H_1(X, m_0)$。

(2)计算 $\omega'=e(P_{pub}, X+h_1'Q_A)$。

(3)验证等式 $m_0=c\oplus H_2(\omega')$。如果等式成立，则认定 σ 是 Alice 对消息 m_0 的有效密文。

如果 σ 是关于 m_0 的有效密文，则 $\omega'=e(P_{pub}, X+h_1'Q_A)=e(P_{pub}, (r+h_1')Q_A)=e(Z,P)$，因此，第(2)步得到的是正确的 ω' 值。该攻击的正确性得到验证，即文献[9]方案不具有语义安全性。

3.2 通用伪造攻击

给出一个针对文献[9]方案的通用伪造(universal forgery)攻击。

给定任何一个身份为 ID_A 的发送者，一个消息 m 和 n 个接收者的身份 $ID_1, ID_2,\cdots, ID_n$，伪造者执行以下操作：

(1)选择 $r\in \mathbb{Z}_q^*$，计算 $X=rQ_A$ 和 $h_1=H_1(X, m)$。

(2)计算 $U=rP$, $\omega=e(P_{pub}, X+h_1Q_A)$, $c=m\oplus H_2(\omega)$和 $W=\omega\theta^r$。

(3)对于 i=1,2,…,n，以正常 Signcrypt 算法中的方式计算 T_i，即 $T_i=rH_1(ID_i)+rR$。

(4)设定密文为 $\sigma=(c, U, X, W, T_1,\cdots, T_n, \Lambda)$，其中，Λ具有正常功能。

可以验证该伪造的密文是有效的，且与合法发送者生成的密文是不可区分的。因此，文献[9]方案是可伪造的。

4 改进方案及其安全性分析

基于文献[7]方案，本文提出一个新的多接收者基于身份签密方案，具体过程如下：

(1)Setup。给定安全参数 k，PKG 选择阶同为素数 q 的循环加法群 G_1 和乘法群 G_2，G_1 的生成元 P，一个双线性映射 e: $G_1\times G_1\to G_2$ 和 3 个哈希函数 H_1:{0, 1}*→G_1, H_2: {0,1}*×$G_2\to \mathbb{Z}_q$ 和 H_3: $G_2\to\{0, 1\}^{l+k}$，其中，l 是待签密消息的比特长度；k 是 G_1 中元素的比特长度。PKG 选取主密钥 $s\in Z_q^*$ 和 $R\in G_1^*$，计算 $P_{pub}=sP$ 和 $\theta=e(R, P_{pub})$。PKG 发布系统参数$(G_1,G_2,P, P_{pub},R,\theta,e,H_1,H_2,H_3)$并秘密保管 s。

(2)Keygen。给定输入身份 ID_U，PKG 计算公钥 $Q_U=H_1(ID_U)$ 和对应的私钥 $D_U=sQ_U$。

(3)Signcrypt。为了发送消息 m 给 n 个接收者 $ID_1, ID_2,\cdots, ID_n$，身份为 ID_A 的发送者 Alice 执行如下操作：

1)选择 $k_1,k_2\in \mathbb{Z}_q^*$。

2)计算 $r=e(P,P)^{k_1}$, $V=k_2P$, $h=H_2(m,r)$和 $U=hD_A+k_1P$。

3)计算 $w=e(P_{pub}, k_2R)$, $c=(m||U)\oplus H_3(w)$，对于 i=1,2,…,n，计算 $T_i=k_2H_1(ID_i)+k_2R$。

之后，Alice 设定密文为 $\sigma=(c,r,V,T_1,\cdots,T_n,\Lambda)$，Λ是一个标签，用来描述 T_i 与 ID_i 的关联。

(4)Designcrypt。从 Alice 收到密文 σ 后，每个接收者 ID_i 执行如下操作：

1)计算 $w=e(V, D_i)^{-1}\cdot e(P_{pub}, T_i)$和 $m||U=c\oplus H_3(w)$。

2)计算 $Q_A=H_1(ID_A)$和 $h=H_2(m, r)$。

3)验证等式 $r=e(U, P)e(P_{pub}, Q_A)^{-h}$。如果等式成立，则输出消息 m，并认定 σ 有效。否则输出特殊字符⊥，表示 σ 不是有效的密文。

本节提出的方案基于文献[7]基于身份的签密方案。根据文献[7]中的安全性结论，分析本文方案的安全性。

定理 1 本文提出的多接收者基于身份签密方案具有语义安全性。

证明：与文献[7]中的定理 1 类似，将本方案的语义安全性规约到群中的双线性 Diffie-Hellman(BDH)问题。给定一个随机的 BDH 问题实例(P, aP, bP, cP)，挑战者设定 $P_{pub}=cP$, $R=bP$，并以与文献[7]中定理 1 类似的方法为攻击者模拟 H_1,H_2, H_3,Keygen,Signcrypt 和 Designcrypt 预言机并挑战密文。根据攻击者的输出，挑战者最终输出 $e(P, P)^{abc}$ 的值。因此，如果 BDH 问题是困难的，则本方案是语义安全的。

定理 2 本文提出的多接收者基于身份签密方案具有存在不可伪造性。

证明：攻击者如果能伪造一个本方案的有效密文，就能伪造一个文献[7]方案的密文。根据文献[7]中定理 2 可知，此时能伪造一个 Hess 方案的签名。由于 Hess 的基于身份签名方案在适应性选择身份和消息攻击下是不可伪造的，因此本文提出的多接收者基于身份签密方案是不可伪造的。

参考文献

[1] Zheng Yuliang. Digital Signcryption or How to Achieve Cost (Signature & Encryption)<<Cost(Signature)+Cost(Encryp-tion)[C]// Proc. of Conf. on Advances in Cryptology-Crypto. [S. l.]: ACM Press, 1997: 165-179.

[2] Baek J, Steinfeld R, Zheng Yuliang. Formal Proofs for the Security of Signcryption[J]. Journal of Cryptology Archive, 2007, 20(2): 203-235.

[3] Malone-Lee J. Identity Based Signcryption[EB/OL]. (2002-07-19). http://eprint.iacr.org/2002/098.

[4] 耿 莉, 王尚平, 周 峰, 等. 一种新的基于身份的签密方案[J]. 计算机工程, 2004, 30(19): 52-54.

[5] 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.

[6] 黄欣沂, 张福泰, 伍 玮. 一种基于身份的环签密方案[J]. 电子学报, 2006, 32(2): 263-266.

[7] 余昭平, 康 斌. 基于 Hess 签名的公开可验证签密方案[J]. 计算机工程, 2008, 34(3): 199-201.

[8] Duan S, Cao Z. Efficient and Provably Secure Multi-receiver Identity-based Signcryption[C]//Proc. of Australasian Conference on Information Security and Privacy. [S. l.]: Springer-Verlag, 2006: 195-206.

[9] Yu Yong, Yang Bo, Huang Xinyi, et al. Efficient Identity-based Signcryption Scheme for Multiple Receivers[C]//Proc. of ATC'07. [S. l.]: Springer-Verlag, 2007.

[10] Chen Liqun, Malone-Lee J. Improved Identity-based Signcryp-tion[C]//Proc. of Conf. on Public Key Cryptography. [S. l.]: Springer-Verlag, 2005: 362-379.

编辑 陈 晖