# 对两个可转变认证加密方案的分析和改进

张串绒[①②] 傅晓彤[①] 肖国镇[①]
[①](西安电子科技大学计算机网络与信息安全教育部重点实验室 西安 710071)
[②](空军工程大学电讯工程学院 西安 710077)

**摘 要** 该文对可转变认证加密进行了研究，指出了Wu-Hsu(2002)方案和Huang-Chang(2003)方案中存在的问题，分别给出了这两个方案的改进方案，很好地解决了认证加密方案的公开验证问题。

**关键词** 认证加密，签名，公开验证，机密性
**中图分类号**：TN918.1 **文献标识码**：A **文章编号**：1009-5896(2006)01-0151-03

# Cryptanalysis and Improvement of Two Convertible Authenticated Encryption Schemes

Zhang Chuan-rong[①②] Fu Xiao-tong[①] Xiao Guo-zhen[①]
[①] (*Key Lab. of Computer Network and Information Security of Ministry of Education, Xidian Univ., Xi´an* 710071, *China*)
[②] (*Telecomm. Eng. Institute, Air force Engineering Univ., Xi´an* 710077, *China*)

**Abstract** Convertible authenticated encryption schemes are studied in this paper. The problems in Wu-Hsu's scheme (2002) and Huang-Chang's scheme (2003) are pointed out. Furthermore the improvements of the two schemes are given; for that, the public verification of authenticated encryption schemes is solved as well.

**Key words** Authenticated encryption, Signature, Public verify, Confidentiality

## 1 引言

在网络通信中，消息常常同时需要保密和认证，实际中实现这一目标的方法是使用密码学的认证加密方案。然而由于消息在被签名的同时也被加密，认证加密方案的有效性只能由意定的接受者来验证，方案本身并不能提供公开验证功能，而在许多实际应用中公开验证又是必不可少的。为了解决这个问题，Araki等提出了一个方案[1]，该方案在必要时可转变为一般的签名方案以实现公开验证。文献[2]指出在Araki方案中，签名的转变需要签名者的合作且所需额外的计算和传输代价较大，进而提出了一个新的方案——Wu-Hsu方案，克服了Araki方案中的问题。随后，文献[3]又给出了一个对Wu-Hsu方案的改进方案——Huang-Chang方案。本文对这些可转变认证加密方案进行了分析研究，发现了其中存在新的问题，指出了相应的解决办法，同时分别给出了对Wu-Hsu方案和Huang-Chang方案的改进方案。

## 2 Wu-Hsu方案[2]和Huang-Chang方案[3]

### 2.1 Wu-Hsu 方案

系统参数： $p$是一个大素数，$q$是$p-1$的一个大素因子，$g\in Z_{p^*}$是$q$阶元素，$x_a\in Zq$是发送者Alice的私钥，$y_a=g^{x_a} \bmod p$是Alice的公钥，类似地，$x_b$和$y_b$分别是接受者Bob的私钥和公钥，hash是一个单向散列函数。

设Alice要发送消息$m$给Bob，那么执行以下操作:

Alice：随机选取整数$k\in Z_q^*$，计算

$$r_1=m(h(y_b{}^k \bmod p))^{-1} \bmod p$$

$$r_2=h(m,h(g^k \bmod p)) \bmod p$$

$$s=k-x_a r_2 \bmod q$$

Alice将$(r_1, r_2, s)$发送给Bob

Bob：恢复消息$m$

$$m=h((g^s y_a{}^{r_2})^{x_b} \bmod p) r_1 \bmod p \tag{1}$$

并检验$m$的冗余，若满足，再检验方程

$$r_2=h(m,h(g^s y_a{}^{r_2} \bmod p)) \bmod q \tag{2}$$

若成立，则签名有效。

当以后发生纠纷，签名者Alice否认自己的签名时，Bob可启用$m$的转变签名$(r_2, s)$来证明Alice的不诚实，即通过式(2)任何人可以验证签名的有效性。

2004-07-20 收到, 2004-12-20 改回
国家自然科学基金重大项目(90104005)和“十五”预研项目(41001040102)资助课题

Wu-Hsu 方案的确解决了 Araki 方案存在的问题，它不再需要签名者的合作即可实现公开验证并且不需象 Araki 方案那样的额外计算。但文献[3]认为 Wu-Hsu 方案没有考虑如果攻击者知道了消息 $m$，也会很容易地将签名转变为一般签名从而带来混乱，为此给出了 Wu-Hsu 方案的一个改进方案如下。

### 2.2 Huang-Chang 方案

系统参数同 Wu-Hsu 方案。如果 Alice 要发送消息 $m$ 给 Bob，那么执行以下操作:

Alice随机选取$k \in Z_P^*$,计算

$$c = my_b^{q-k} \bmod p$$

$$r=h(m, y_b, g^k) \bmod q$$

$$s=k - x_a r \bmod q,$$

Alice 将$(c, r, s)$给 Bob.

Bob 回复 $m$：

$$m = c(y_a^r g^s)^{x_b} \bmod p \tag{3}$$

若等式

$$r = h(m, y_b, y_a^r g^s) \bmod q \tag{4}$$

成立，则签名有效。Bob 接受秘密消息 $m$ 和 Alice 的签名。

当 Alice 否认自己的签名时，Bob 用消息的转变签名$(r, s)$可证明 Alice 的不诚实。通过验证式(4)，任何人都可证明签名的有效性。

## 3 存在的问题和改进方案

### 3.1 存在的问题

文献[3]称，用 Huang-Chang 方案，只有意定的接受者才能将 $m$ 和转变签名给任意的验证者来验证签名的有效性。关于这点，本文认为并非该方案才有，Wu-Hsu 方案本来就是如此，因为只有意定的接受者用自己的私钥才能恢复出 $m$。另外关于攻击者知道消息 $m$ 的问题，本文认为既然是公开验证，就是任何人都可验证，并没有也不应把任何人除外包括攻击者。转变签名的目的只是为了公开验证，攻击者能转变签名并不能影响什么，也不会因此产生任何混乱。

本文认为Huang-Chang方案，包括Wu-Hsu方案有另一个重要的问题需要考虑。回顾Araki方案，在签名转变阶段，Alice将只有她才能计算出的$u = (sx_a r_2^{-1} + j) \bmod q$ 和签名$(r_2$，$s$，$J)$给验证者来实现公开验证；而在Huang-Chang方案和Wu-Hsu方案中，签名转变阶段是Bob 将只有他可恢复的消息$m$ 给了验证者，来实现公开验证。然而，Huang-Chang方案和Wu-Hsu方案都是认证加密方案，不同于单纯的签名只要认证而不考虑消息的机密性。认证加密方案是要实现两项功能，即除了认证功能还有保密功能，为了实现认证而破坏保密性是不符合认证加密的安全要求的。Huang-Chang方案和Wu-Hsu方案在签名转变阶段都是将要保密的消息给了验证者以实现公开验证，这违背了认证加密的目的。当然，如果公开验证是很长时间以后才进行，消息已无需保密，在这种情况下Huang-Chang方案和Wu-Hsu方案是可行的，这应另当别论。下面针对Wu-Hsu方案和Huang-Chang方案公开验证破坏消息的机密性的问题，分别提出了改进方案。

### 3.2 改进方案

在Wu-Hsu方案中，转变签名是$(r_2, s)$，验证者拥有消息$m$及其它一些公开信息。为了公开验证不破坏消息的机密性和提高验证的有效性，本文对Wu-Hsu方案做了如下改进：(1)让验证式中含有接受者Bob的公钥，这样公开验证就能证明接受者的有效性；(2)将$r_2$的计算式中的$m$改为$h(m)$,即

$$r_2 = h(h(m), y_b, h(g^k \bmod p)) \bmod p \tag{5}$$

这样，在出现纠纷，Alice 否认自己的签名时，Bob将$h(m)$和转变签名$(r_2, s)$给验证者，任何人通过

$$r_2 = h(h(m), y_b, h(g^s y_a^{r_2} \bmod p)) \bmod q$$

便可验证签名的有效性。这样的验证，不泄漏消息 $m$，且其正确性、其它安全性、有效性与原方案相同。

对于 Huang-Chang 方案除了主要解决公开验证泄漏消息 $m$ 的问题外，方案中还有一个数学问题需要指出，就是加密时，方案中的计算式是 $c = my_b^{q-k} \bmod p$，实际上这里必须加上一个条件 $q-$k 与 $p-1$ 互素。如果没有这个条件，密文可能等于明文，加密就失去意义。然而，Alice 随机选取的 $k$ 未必能满足上述条件，为此，可采取下面的两种方法得到满足条件的 $k$。一种是，如果$(q-k,\ p-1)\neq 1$(或者 $q-k=1 \bmod p-1$)，Alice 就必须重新随机选取 $k$，直到满足互素的条件为止；还有一种办法就是当 $q-k$ 与 $p-1$ 不互素时 Alice 计算 $Q = q-k/(q-k, p-1)$，看 $Q$ 与 $p-1$ 是否互素,不互素，上式中再以 $Q$ 代替 $q-k$ 计算下一个 $Q$；如此直到某个 $Q$ 与 $p-1$ 互素，这时，让 $q-$k 等于最后算得的该 $Q$，算出 $k$，即为满足上述互素条件的 $k$。

下面来修改 Huang-Chang 方案公开验证中的问题。在 Huang-Chang 方案中的公开验证阶段，Bob 将消息 $m$ 和转变签名$(r, s)$给了验证者，本文对此做如下修改。令

$$r = h(c, y_b, g^k) \bmod q$$

这样 Bob 只要将密文 $c$ 和转变签名$(r, s)$给验证者，任何人就可通过

$$r = h(c, y_b, y_a{}^r g^s) \bmod q$$

验证签名的有效性。

## 4　结束语

可转变认证加密方案是为了解决认证加密中的公开验证问题提出的。当出现纠纷，签名者否认自己的签名时，可将可转变认证加密方案中的签名转变为一般签名来实现公开验证。但当消息的机密性不容破坏时，已有文献 Huang-Chang 方案和 Wu-Hsu 方案中的可转变签名公开验证就不再适用。本文提出的修改方案正弥补了 Huang-Chang 方案和 Wu-Hsu 方案的这种不足，一方面既克服了 Araki 方案中转变验证需要签名者合作的麻烦，另一方面又改变了 Huang-Chang 方案和 Wu-Hsu 方案需要将消息泄漏给第三者的弊端，是一种不泄漏消息机密性的真正的可实现公开验证的认证加密方案。

## 参 考 文 献

[1] Araki S, Uehara S, Imamura K. Convertible limited verifier signature based on horster's authenticated encryption. 1998 Symposium on Cryptography and Information Security. Hamanako, Japan, 32 – 36.

[2] Wu T S, Hsu C L. Convertible authenticated encryption scheme. *The Journal of Systems and Software*, 2002，62(3): 205 – 209.

[3] Huang Hui-Feng，Chang Chin-Chen. An efficient convertible authenticated encryption scheme and its variant. ICICS 2003, LNCS 2836, Berlin, Heidelberg Pringer-Verlag 2003: 382 – 392.

张串绒：　女，1965年生，博士生，副教授，研究方向为应用数学、密码学与信息安全.

傅晓彤：　女，1977年生，博士生，研究方向为公钥密码学.

肖国镇：　男，1934年生，博士生导师，教授，研究方向为密码学与信息安全.