第35卷 第20期 计 算 机 工 程 2009年10月
Vol.35 No.20 Computer Engineering October 2009
·安全技术· 文章编号：1000—3428(2009)20—0165—02 文献标识码：A 中图分类号：TN918

叛逆者追踪方案的密码学分析

张建中[1]，王永峰[1]，王翠玲[2]
(1. 陕西师范大学数学与信息科学学院，西安 710062；2. 哈尔滨理工大学测控技术与通信工程学院，哈尔滨 150080)

摘 要：对一种叛逆者追踪方案提出安全性分析，指出它存在的安全缺陷有被撤销的叛逆者可以在合法用户的帮助下继续解密新密文及合法用户可以合谋伪造有效的解密密钥。提出伪造攻击方案，并给出方案被攻击的原因。指出方案的一个设计错误，说明该方案在实际操作上是不可行的。

关键词：叛逆者追踪；RSA 算法；合谋攻击

Cryptanalysis of Traitor Tracing Scheme

ZHANG Jian-zhong[1], WANG Yong-feng[1], WANG Cui-ling[2]
(1. College of Mathematics and Information Science, Shaanxi Normal University, Xi'an 710062;
2. School of Measurement-Control Tech. & Communications Engineering, Harbin University of Science & Technology, Harbin 150080)

【Abstract】Cryptanalysis of a traitor tracing scheme shows that it exists follow security deficiencies: the revoked traitor can decrypt new ciphertext under the help of legitimate user; legitimate users can forge effective decryption key if they conspire. This paper proposes forgery attack scheme and gives the reason why it is attacked. This paper points out one mistake in designation of the scheme, which explains it is not feasible in the actual operation.

【Key words】 traitor racing; RSA algorithm; colluding attack

1 概述

数据提供商(Data Supplier, DS)在开放式网络中销售数字产品时，为了防止非授权用户获取网络数据，通过广播信道提供加密信息。授权用户用自己的密钥先将加密数据包头中的会话密钥解密，然后用得到的会话密钥解密加密数据。如恶意的授权用户将自己的密钥泄露给别的非法用户使用，或者某些授权用户先共谋制造出密钥然后让非法用户使用，那么这些恶意的授权用户就称为叛逆者，非法用户称为盗版者，通过盗版者的解码器分析出叛逆者的工作称为叛逆者追踪。

文献[1]首先提出叛逆者追踪的概念。随后文献[2]提出了非对称叛逆者追踪的概念，解决了对称方案中存在的问题，即只有授权用户自己知道自己的密钥，不诚实的 DS 不能诬陷合法诚实用户，并使得 DS 可以明确地向第三方证明叛逆者参与盗版的事实。文献[3]考虑了叛逆者撤销的问题。目前提出的叛逆者追踪方案大多数是基于离散对数难解问题，而基于大整数分解难解问题的叛逆者追踪方案[4-9]为数不多。

文献[9]提出的方案具有撤销叛逆者和增加用户的优点。本文对该方案提出密码学分析，发现方案存在安全缺陷。

2 方案

2.1 系统参数

设系统中用户数为 n，DS 选取 RSA 算法的公开密钥 (e,N)，秘密钥为 d。

2.2 初始化过程

DS 进行以下操作：

(1)秘密选取 n 个互不相同的整数 $t_{11},t_{12},\cdots,t_{1n}$，使得这 n 个数满足以下 2 个条件：

1) $(t_{1i},\varphi(N))=1$；

2) $t_{2i}=d-t_{1i}(\mathrm{mod}\,\varphi(N)),\gcd(t_{2i},\varphi(N))=1,i=1,2,\cdots,n$。

(2)计算 $T_1=t_{11}t_{12}\cdots t_{1n}r_1(\mathrm{mod}\,\varphi(N)),T_2=t_{21}t_{22}\cdots t_{2n}r_2(\mathrm{mod}\,\varphi(N))$。其中，$r_1,r_2$ 为秘密选取的 2 个随机素数；T_1,T_2 由 DS 私藏。

(3)计算 $d_{1i}=t_{1i}T_1^{-1}(\mathrm{mod}\,\varphi(N)),d_{2i}=t_{2i}T_2^{-1}(\mathrm{mod}\,\varphi(N))$。

(4)通过安全信道将 (d_{1i},d_{2i}) 秘密发送给用户 i 作为其个人密钥，并记录用户 i 与 (d_{1i},d_{2i}) 的关系。

2.3 加密

DS 选取会话密钥 $s(1<s<N)$，计算密文 $C=(c_1,c_2)=(s^{T_1e}\bmod N,s^{T_2e}\bmod N)$，然后将 C 广播发送给所有用户。

2.4 解密

用户 i 接收到密文 C 后，用其个人密钥 (d_{1i},d_{2i}) 进行解密，计算出会话密钥 s。具体计算过程如下：

$$c_1^{d_{1i}}c_2^{d_{2i}}=s^{T_1ed_{1i}}s^{T_2ed_{2i}}(\mathrm{mod}\,N)=s^{t_{1i}e+t_{2i}e(\mathrm{mod}\,\varphi(N))}(\mathrm{mod}\,N)=$$
$$s^{ed(\mathrm{mod}\,\varphi(N))}(\mathrm{mod}\,N)=s(\mathrm{mod}\,N)$$

2.5 叛逆者追踪

一旦发现盗版，DS 从没收的盗版解码器中获得 (d_{1i},d_{2i})，可以断定用户 i 是叛逆者。

2.6 叛逆者个人密钥的撤销和新用户的增加

(1)若确立用户 i 为叛逆者，则 DS 重新选择 2 个随机素数 r_1' 和 r_2'，用于更新 T_1 和 T_2：

基金项目：国家自然科学基金资助项目(10571113)；陕西省自然科学研究计划基金资助项目(2004A14)；陕西省教育厅科学研究计划自然科学基金资助项目(07JK375)

作者简介：张建中(1960－)，男，教授、博士，主研方向：密码学，信息安全，电子商务；王永峰、王翠玲，硕士研究生

收稿日期：2009-03-18 **E-mail：**d2000d@163.com

$T_1' = t_{11}t_{12}\cdots t_{1(i-1)}t_{1(i+1)}\cdots t_{1n}r_1' (\mathrm{mod}\,\varphi(N))$

$T_2' = t_{21}t_{22}\cdots t_{2(i-1)}t_{2(i+1)}\cdots t_{2n}r_2' (\mathrm{mod}\,\varphi(N))$

计算 $\alpha_1 = t_{1i}r_1(r_1')^{-1} \bmod \varphi(N), \alpha_2 = t_{2i}r_2(r_2')^{-1} \bmod \varphi(N)$，并将 (α_1,α_2) 广播给其他合法用户。用户 $j(j \neq i)$ 收到数据后，计算 $d_{1j}' = d_{1j}\alpha_1$，$d_{2j}' = d_{2j}\alpha_2$，(d_{1j}', d_{2j}') 便是用户 j 的新的个人密钥。这样一来，由于 T_1, T_2 的更新，叛逆者 i 不能解密新的密文，即其解密能力被废除。而对于其户 j 而言，设新的密文为 C'，则 $C' = (c_1', c_2') = (s^{T_1'e}, s^{T_2'e})$，利用新的个人密钥 (d_{1j}', d_{2j}') 进行解密计算从而获取会话密钥 s，其简略步骤为

$$(c_1')^{d_{1j}'}(c_2')^{d_{2j}'} = s^{T_1'ed_{1j}'}s^{T_2'ed_{2j}'} (\mathrm{mod}\,N) = s^{ed \bmod \varphi(N)} (\mathrm{mod}\,N) = s(\mathrm{mod}\,N)$$

(2)若有一个新用户 $n+1$ 要加入该系统，则 DS 首先秘密选取一个整数 $t_{1(n+1)}$，使得 $t_{1(n+1)}$ 满足 2.2 节中提到的 2 个条件。同时，重新选择 2 个随机素数 r_1'' 和 r_2'' 来更新 T_1 和 T_2：

$T_1'' = t_{11}t_{12}\cdots t_{1n}t_{1(n+1)}r_1'' (\mathrm{mod}\,\varphi(N))$

$T_2'' = t_{21}t_{22}\cdots t_{2n}t_{2(n+1)}r_2'' (\mathrm{mod}\,\varphi(N))$

计算

$$d_{1(n+1)} = t_{1(n+1)}(T_1'')^{-1} (\mathrm{mod}\,\varphi(N)), d_{2(n+1)} = t_{2(n+1)}(T_2'')^{-1} (\mathrm{mod}\,\varphi(N))$$

其中，$t_{2(n+1)} = d - t_{1(n+1)} (\mathrm{mod}\,\varphi(N))$，并将 $(d_{1(n+1)}, d_{2(n+1)})$ 作为解密密钥发送给用户 $n+1$。计算

$$\beta_1 = r_1(r_1''t_{1(n+1)})^{-1} \bmod \varphi(N), \beta_2 = r_2(r_2''t_{2(n+1)})^{-1} \bmod \varphi(N)$$

并将 (β_1, β_2) 广播给其他所有用户。用户 $i(i = 1,2,\cdots,n)$ 收到数据后计算 $d_{1i}'' = d_{1i}\beta_1$，$d_{2i}'' = d_{2i}\beta_2$，(d_{1i}'', d_{2i}'') 便是用户 i 的新的个人密钥，利用上述解密算法便可以解密增加用户 $n+1$ 后新的密文。

3 伪造攻击

3.1 合法用户协助下会话密钥的解密

叛逆者 i 在被撤销之后，收到合法用户 j 发送的更新后的 (α_1,α_2)，可以计算 $d_{1i}' = d_{1i}\alpha_1, d_{2i}' = d_{2i}\alpha_2$。$(d_{1i}', d_{2i}')$ 对叛逆者而言是有效的解密密钥，而且 DS 不能追踪到 (d_{1i}', d_{2i}') 的具体身份。假设 DS 广播密文 (c_1', c_2')，i 可以利用解密密钥恢复会话密钥 s。

恢复过程如下：

$$(c_1')^{d_{1i}'}(c_2')^{d_{2i}'} = s^{T_1'ed_{1i}'}s^{T_2'ed_{2i}'} (\mathrm{mod}\,N) = s^{(T_1'd_{1i}'+T_2'd_{2i}')e} (\mathrm{mod}\,N) =$$

$$s^{(t_{11}t_{12}\cdots t_{1(i-1)}t_{1(i+1)}\cdots t_{1n}r_1'd_{1i}\alpha_1 (\mathrm{mod}\,\varphi(N))+t_{21}t_{22}\cdots t_{2(i-1)}t_{2(i+1)}\cdots t_{2n}r_2'd_{2i}\alpha_2 \bmod \varphi(N))e} (\mathrm{mod}\,N) =$$

$$s^{(t_{11}t_{12}\cdots t_{1(i-1)}t_{1(i+1)}\cdots t_{1n}r_1'd_{1i}t_{11}r_1(r_1')^{-1} (\mathrm{mod}\,\varphi(N))+t_{21}t_{22}\cdots t_{2(i-1)}t_{2(i+1)}\cdots t_{2n}r_2'd_{2i}t_{21}r_2(r_2')^{-1})e (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N) =$$

$$s^{(t_{11}t_{12}\cdots t_{1(i-1)}t_{1i}t_{1(i+1)}\cdots t_{1n}r_1'd_{1i} (\mathrm{mod}\,\varphi(N))+t_{21}t_{22}\cdots t_{2(i-1)}t_{2i}t_{2(i+1)}\cdots t_{2n}r_2'd_{2i} (\mathrm{mod}\,\varphi(N)))e} (\mathrm{mod}\,N) =$$

$$s^{(T_1d_{1i}+T_2d_{2i} (\mathrm{mod}\,\varphi(N)))e} = s^{(t_{1i}+t_{2i})e} (\mathrm{mod}\,N) = s^{(t_{1i}+t_{2i})e (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N) =$$

$$s^{((t_{1i}+t_{2i}) (\mathrm{mod}\,\varphi(N)))e (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,\varphi(N)) = s^{de (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N) = s(\mathrm{mod}\,N)$$

3.2 新的解密密钥的产生

假设合法用户 U_i, U_j 合谋伪造 $d_1 = 2d_{1i} - d_{1j}$，$d_2 = 2d_{2i} - d_{2j}$，可以证明 (d_1, d_2) 和用户 U_i 的 (d_{1i}, d_{2i}) 不相同，否则用户 U_i, U_j 的解密密钥完全相同，这是不符合叛逆者追踪方案的要求的。若 (d_1, d_2) 和 U_j 的 (d_{1j}, d_{2j}) 完全相同，可以根据注(1)重新伪造一个解密密钥；若 (d_1, d_2) 和其他合法用户(不妨设为 U_s)的解密密钥完全相同，可以对用户 U_s 构成陷害；若 (d_1, d_2) 和任意一个群成员的解密密钥都不相同，DS 不能根据 (d_1, d_2) 追踪到解密者身份。

下证 (d_1, d_2) 是有效的解密密钥。

$$c_1^{d_1}c_2^{d_2} = s^{T_1ed_1}s^{T_2ed_2} (\mathrm{mod}\,N) = s^{T_1e(2d_{1i}-d_{1j})}s^{T_2e(2d_{2i}-d_{2j})} (\mathrm{mod}\,N) =$$

$$s^{2(T_1ed_{1i}+T_2ed_{2i})-(T_1ed_{1j}+T_2ed_{2j})} (\mathrm{mod}\,N) = s^{2(T_1ed_{1i}+T_2ed_{2i})}s^{-(T_1ed_{1j}+T_2ed_{2j})} (\mathrm{mod}\,N) =$$

$$s^{2((t_{1i}+t_{2i}) \bmod \varphi(N))e}s^{-((t_{1j}+t_{2j}) \bmod \varphi(N))e} (\mathrm{mod}\,N) = s^{2de (\mathrm{mod}\,\varphi(N))}s^{-de (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N) =$$

$$s^{de (\mathrm{mod}\,\varphi(N))} (\mathrm{mod}\,N) = s(\mathrm{mod}\,N)$$

注：(1)任意 2 个合法用户在合谋的情况下，可以构造无数个各不相同的有效的解密密钥。只要令

$$d_1 = (k+1)d_{1i} - kd_{1j}, d_2 = (k+1)d_{2i} - kd_{2j}$$

其中，k 是一个正整数。

(2)任意 $k(1 < k < n)$ 个被授权用户也可以合谋伪造有效的解密密钥。

4 被攻击原因

4.1 叛逆者恢复密钥的原因

叛逆者 i 可以恢复解密密钥的主要原因是所有用户的 (α_1,α_2) 是相同的，方案的合法用户可以继续恢复解密密钥，是因为在 $T_1', T_2', \alpha_1, \alpha_2$ 构造上使得 $T_1'\alpha_1 = T_1 \bmod \varphi(N)$, $T_2'\alpha_2 = T_2 \bmod \varphi(N)$ 同时成立。叛逆者 i 在获取 (α_1,α_2) 的前提下，可以继续生成有效的解密密钥 (d_{1i}', d_{2i}')，而且不会被追踪到身份。因为 (d_{1i}', d_{2i}') 并不和叛逆者 i 的身份相对应。要避免这种安全缺陷，在 (α_1,α_2) 构造上要使得叛逆者 i 在得到 (α_1,α_2) 之后仍然不可以解密，或者使得所有用户的 (α_1,α_2) 各不相同，叛逆者在没有得到自己的 (α_1,α_2) 的前提下，利用其他用户的 (α_1,α_2) 不能构造有效的解密密钥。

4.2 合法成员合谋伪造的原因

合法用户 i, j 可以成功解密，是因为等式 $T_1d_{1i} + T_2d_{2i} = t_{1i} + t_{2i} = d (\mathrm{mod}\,\varphi(N))$，$T_1d_{1j} + T_2d_{2j} = t_{1j} + t_{2j} = d (\mathrm{mod}\,\varphi(N))$ 同时成立，在此基础上合法用户 i, j 伪造 (d_1, d_2)。要使得构造有效，必然要满足 $T_1d_1 + T_2d_2 = t_{1i} + t_{2i} = d \bmod \varphi(N)$，所以 $d_1 = 2d_{1i} - d_{1j}, d_2 = 2d_{2i} - d_{2j}$ 是有效伪造。

5 一个设计错误

方案在设计上存在一个错误，在满足 RSA 算法的基础上，下面 2 点不能同时满足：

(1) $(t_{1i}, \varphi(N)) = 1$

(2) $t_{2i} = d - t_{1i} (\mathrm{mod}\,\varphi(N)), \gcd(t_{2i}, \varphi(N)) = 1, i = 1,2,\cdots,n$

由 RSA 算法知 $2 | \varphi(N)$，且 d 是奇数，由条件(1)知 t_{1i} 也是奇数，从而 $2 | d - t_{1i}$。又由 $t_{2i} = d - t_{1i} (\mathrm{mod}\,\varphi(N))$ 知 $2 | t_{2i}$，故 $2 | \gcd(t_{2i}, \varphi(N))$，即 $\gcd(t_{2i}, \varphi(N)) \neq 1$, $i = 1,2,\cdots,n$。所以条件(1)和条件(2)不能同时满足，从而 $T_1^{-1} \bmod \varphi(N), T_2^{-1} \bmod \varphi(N)$ 不可以同时存在，即 d_{1i}, d_{2i} 不同时存在。若 t_{1i}, t_{2i} 同时满足条件(1)和条件(2)，则类似可得 $2 | \gcd(d, \varphi(N))$，从而 $\gcd(d, \varphi(N)) \neq 1$，这与 RSA 算法中 d 的要求是不符合的。

综上所述，发现原方案中的 RSA 算法中 N, e, d 的选取和满足条件(1)和条件(2)的 t_{1i}, t_{2i} 选取是不可以同时成立的，说明方案不具备实际操作性。

6 结束语

本文对文献[9]提出的叛逆者追踪方案实行了伪造攻击，说明该方案是不安全的。被撤销的用户可以在合法用户的帮助下继续生成有效的解密密钥，而且 DS 不可以追踪到解密者身份；多个合法用户可以生成多个有效的解密密钥，从而对其他成员构成陷害或者使得 DS 不可以追踪身份。

(下转第 172 页)