文章编号:1005-0523(2019)04-0119-05

对一个无证书签密方案的攻击与改进

左黎明[1,2],夏萍萍[1,2],林 楠[3]

(华东交通大学 1.理学院;2.系统工程与密码学研究所,江西 南昌 330013;
3.国网江西电力有限公司电力科学研究院,江西 南昌 330096)

摘要:为了简化证书的管理和密钥托管的问题,同时提高无证书签密方案的计算效率和安全性,陈虹等人提出一种可证安全的无证书签密机制,并在随机预言机下证明该机制满足机密性和不可伪造性。通过构造3种攻击算法,证明了陈虹等人所提出的安全机制不能抵抗用户公钥替换攻击、系统主密钥与用户部分公钥泄露攻击、合谋攻击,分析了这些漏洞产生的原因,并提出了改进的修补方案。

关键词:签密;随机预言机;椭圆曲线;机密性;不可伪造性

中图分类号:TP309.2 **文献标志码**:A

1997年,Zheng[1]首次提出签密的概念,传统的签密方案易受到“公钥替换”攻击[2]。1984年Shamir[3]提出一种基于身份的密码体制,公钥由用户的身份信息(用户的学号、手机号、微信号等)直接生成。2008年,Barbosa等人[4]提出了一种基于无证书的签密方案,该方案融合了无证书密码体制与签密体制。基于双线性对的[5-7]签密方案相对于无对映射的方案[8-10]较慢。陈虹等人[11]基于汤永利等人[12]构造的方案基础上,提出了一种可证安全的基于无对映射的无证书签密方案,并在随机预言模型下基于计算椭圆曲线上的离散对数困难问题证明了方案的机密性和不可伪造性,但我们研究发现陈虹等人[11]的方案安全性值得商榷,存在三种类型的攻击,本文给出了这三种类型攻击的具体方法、产生原因和改进方案。

1 原方案[11]回顾

1) 系统建立:给定安全参数 k,选择阶为素数 q 的椭圆曲线 $E(F_p)$ 上群 G(生成元为 P),选择哈希函数 $H_1:\{0,1\}^*\rightarrow Z_q^*$,$H_2:\{0,1\}^*\rightarrow Z_q^*$,$H_3:Z_q^*\times Z_q^*\{0,1\}^*\rightarrow Z_q^*$。密钥生成中心(key generator center,KGC)保存主密钥 s,计算公钥 $P_{pub}=sP$。公开系统参数:$params=\{p,q,G,P,P_{pub},H_1,H_2,H_3\}$。

2) 部分密钥提取:KGC选择 $r_i\in Z_q^*$,计算用户 ID_i 的部分私钥 $R_i=r_iP$,部分公钥 $D_i=r_i+sH_1(ID_i,R_i)$,将 (R_i,D_i) 返回给用户。

3) 秘密值选择:随机选择 $x_i\in Z_q^*$ 作为用户的秘密值。

4) 私钥生成:生成用户的私钥对 (x_i,D_i),用户 A 的私钥为 $SK_A=(x_A,D_A)$,用户 B 的私钥为 $SK_B=(x_B,D_B)$。

5) 公钥生成:计算 $X_i=x_iP$,生成公钥对 (X_i,R_i),可得用户 A、用户 B 的公钥分别为 $PK_A=(X_A,R_A)$,$PK_B=(X_B,R_B)$。部分私钥的正确性由等式 $R_i+H_1(ID_i,R_i)P_{pub}=D_iP$ 来验证。

6) 签密:发送者 A 对消息 m 进行签密后发送给接收者 B,具体步骤如下:

① 发送者 A 随机选择 $t\in Z_q^*$,计算 $T=tP$;

收稿日期:2018-04-20

基金项目:国家自然科学基金项目(11361024);国网江西省电力有限公司科技项目(52182017001L);江西省教育厅科技项目(GJJ161417,GJJ170386);江西省交通运输厅科技项目(2017D0037)

作者简介:左黎明(1981—),男,副教授,研究方向为信息安全及非线性系统。

② 计算 $h_1=H_1(ID_B,R_B)$,$h_2=H_3(m,T,R_A,X_A)$,$u=t+x_Ah_1+D_Ah_2$;

③ 计算 $K_1=x_A,X_B,K_2=(R_B+P_{pub}h_1)D_A$,$V_A=H_3(K_1,K_2)$,$c=V_A\oplus m$,其中 c 为 m 的密文;

④ 发送者 A 向接收者 B 发送签密密文 $\sigma=(c,h_2,u)$。

7) 解签密:接收者 B 收到后 $\sigma=(c,h_2,u)$,进行解签密的步骤如下:

① 计算 $h_1=H_1(ID_A,R_A)$和 $T'=uP-X_Ah_1-R_Ah_2-P_{pub}h_1'h_2$;

② 计算 $V_B=H_3(X_Ax_B,(R_A+P_{pub}h_1')D_B)$,恢复明文 $m=V_B\oplus c$;

③ 计算 $h_2'=H_2(m,T',R_A,X_A)$,若 $h_2'=h_2$,输出明文 m;否则拒绝签密。

2 对原方案的攻击与分析

2.1 攻击 1

假设用户 A 为签密者, 用户 B 为攻击者,B 作为签密接收者曾经与 A 完成过一次正常的签密过程,获得一个关于消息 m 的有效签密 $\sigma=(c,h_2,u)$。B 知道 A 的部分密钥 D_A,但不知道用户自己选择的秘密值 x_A,那么 B 可以伪造一个 A 发送给 B 的关于任意消息$\hat{m}$的有效签密$\hat{\sigma}$,以下为攻击过程:

1) B 利用等式 $u=t+x_Ah_1+D_Ah_2$ 计算 $t+x_Ah_1=u-D_Ah_2$;

2) 因为 $uP=tP+x_Ah_1P+D_Ah_2P$,$h_1=H_1(ID_B,R_B)$,所以 B 可以计算出 $T=uP-h_1X_A+h_2D_AP$,从而计算与新的消息$\hat{m}$相关的$\hat{h}_2=H_2(\hat{m},T,R_A,X_A)$;

3) B 计算$\hat{u}=u-D_Ah_2+D_A\hat{h}_2$(即$\hat{u}=t+x_Ah_1+D_A\hat{h}_2$);

4) 因为密钥 $V_A=V_B=H_3(x_Ax_BP,D_AD_BP)$,所以 B 可以计算:$V_A=H_3(x_Bx_B,D_AD_BP)$,于是 B 最终可以计算密文:$\hat{c}=V_A\oplus\hat{m}$,伪造出 A 的关于$\hat{m}$的新签密$\hat{\sigma}=(\hat{c},\hat{h}_2,\hat{u})$。新的签密$\hat{\sigma}$可以通过解签密验证。

2.2 攻击 2

与攻击 1 类似,假设攻击者 B 曾经作为签密接收者与 A 完成过一次正常的签密过程,获得一个关于消息 m 的有效签密 $\sigma=(c,h_2,u)$。B 知道系统主密钥 s,但不知道用户自己选择的秘密值 x_A,那么 B 可以伪造一个 B 发送给的任意消息$\hat{m}$的有效签密$\hat{\sigma}$,以下为攻击过程:

1) B 随机选一个$\hat{r}\in Z_q^*$,计算$\hat{R}_A=\hat{r}P$,$\hat{D}_A=\hat{r}+\hat{s}H_1(ID_A,\hat{R}_A)$,并声称 A 的公钥为$(X_A,\hat{R}_A)$;

2) B 利用等式 $u=t+x_Ah_1+D_Ah_2$ 计算 $t+x_Ah_1=u-D_Ah_2$;

3) 因为 $uP=tP+x_Ah_1P+D_Ah_2P$,$h_1=H_1(ID_B,R_B)$,所以 B 可以计算出 $T=uP-h_1X_A+h_2D_AP$,从而计算与新的消息$\hat{m}$相关的$\hat{h}_2=H_2(\hat{m},T,R_A,X_A)$;

4) B 计算$\hat{u}=u-D_Ah_2+\hat{D}_A\hat{h}_2$ (即$\hat{u}=t+x_Ah_1+\hat{D}_A\hat{h}_2$);

5) 因为密钥 $V_A=V_B=H_3(x_Ax_BP,D_AD_BP)$,所以 B 可以计算:$V_A=H_3(x_BX_B,\hat{D}_AD_BP)$,于是 B 最终可以计算密文:$\hat{c}=V_A\oplus\hat{m}$,伪造出 A 的关于$\hat{m}$的新签密$\hat{\sigma}=(\hat{c},\hat{h}_2,\hat{u})$。新的签密$\hat{\sigma}$可以通过验证。

2.3 攻击 3

假设用户 A 为签密者,用户 B 和用户 C 为合谋攻击者,B 作为签密接收者曾经与 A 完成过一次正常的签密过程,获得一个关于消息 m 有效的签密密文 $\sigma=(c,h_2,u)$。B 知道用户自己选择的秘密值 x_A,但不知道 A 的部分密钥 D_A,那么用户 B 和用户 C 可以合谋伪造一个 A 发送给 C 关于消息 m 的有效签密$\hat{\sigma}$,以下为攻击过程:

1) B 计算 $h_1=H_1(ID_B,R_B)$,再利用等式 $u=t+x_Ah_1+D_Ah_2$ 计算 $t+D_Ah_2=u-x_Ah_1$;

2) B 计算$\hat{h}_1=H_1(ID_C,R_C)$,$\hat{u}=u-x_Ah_1+x_A\hat{h}_1$(即$\hat{u}=t+x_A\hat{h}_1+D_Ah_2$);

3) B 把$(m,h_2,\hat{u})$发送给 C;

4）C 计算 $Y_A=R_A+H_1(ID_A,R_A)P_{pub}$，因为 A 与 C 密钥 $\hat{V}_A=\hat{V}_C=H_3(x_Ax_CP,D_AD_CP)$，所以 C 可以计算：$\hat{V}_A=H_3(x_CX_A,D_CY_A)$。于是 B 最终可以计算密文：$\hat{c}=\hat{V}_A\oplus m$，伪造出 A 的关于 $\hat{m}$ 的新签密 $\hat{\sigma}=(\hat{c},\hat{h}_2,\hat{u})$。新的签密 $\hat{\sigma}$ 可以通过解签密验证。

2.4　原方案的脆弱性分析

原方案的脆弱性主要体现在两个方面：首先原方案用来加密明文的密钥生成过于简单，与每次签密中选择的公开参数没有任何关系，每次是一样的。其次，哈希函数的设计不合理。例如对原方案的攻击 1 和攻击 2 能够成功的原因在于原方案在计算 $u=t+x_Ah_1+D_Ah_2$ 时，其中的 $h_1=H_1(ID_B,R_B)$ 与当前的消息 m 和选择的参数无关联，攻击 3 能够成功的原因在于原方案在计算 $u=t+x_Ah_1+D_Ah_2$ 时，其中的 $h_2=H_2(m,T,R_A,X_A)$ 与当前签密接收者信息无关联。

3　改进方案及其安全性分析

3.1　改进方案

鉴于以上分析，改进方案如下：

1）系统参数建立；

2）用户部分密钥生成；

3）秘密值生成；

4）用户私钥生成；

5）用户公钥生成与原方案相同；

6）签密：当发送者 A 对明文 m 进行签密发送给接受者 B 时，执行以下步骤：

① 用户 A 随机选择 $t\in Z_q^*$，计算 $T=tP$；

② 计算 $h_1=H_1(m,ID_B,R_B)$，$h_2=H_2(m,T,R_A,X_A,R_B,X_B)$，$u=t+x_Ah_1+D_Ah_2$；

③ 计算 $KEY=h_2x_AX_B+D_A(R_B+H_1(ID_B,R_B)P_{pub})$，$V_A=H_3(KEY)$，加密明文 $c=V_A\oplus m$；

④ 用户 A 向用户 B 发送签密密文 $\sigma=(c,h_2,u)$。

7）解签密：用户 B 收到 $\sigma=(c,h_2,u)$ 后，执行以下步骤：

① 计算 $KEY'=h_2x_BX_A+D_B(R_A+H_1(ID_A,R_A)P_{pub})$，$T'=uP-X_Ah_1-R_Ah_2-P_{pub}h_1'h_2$；

② 计算 $V_B=H_3(KEY')$，恢复明文 $m'=V_B\oplus c$；

③ 计算 $h_2'=H_2(m',T',R_A,X_A,R_B,X_B)$，若 $h_2'=h_2$，则接受签密 $\sigma=(c,h_2,u)$，否则拒绝签密。

3.2　正确性证明

改进方案的正确性分析如下：

因为

$$\begin{aligned}V_A&=H_3(h_2x_AX_B+D_A(R_B+H_1(ID_B,R_B)P_{pub}))\\&=H_3(h_2x_AX_B+(r_A+sH_1(ID_A,R_A))(R_B+H_1(ID_B,R_B)P_{pub}))\\&=H_3(h_2x_AX_B+r_Ar_BP+P_{pub}(H_1(ID_B,R_B)r_A+H_1(ID_A,R_A)r_B+sP_{pub}H_1(ID_A,R_A)H_1(ID_B,R_B))\\V_B&=H_3(h_2x_BX_A+D_B(R_A+H_1(ID_A,R_A)P_{pub}))\\&=H_3(h_2x_AX_B+(r_B+sH_1(ID_B,R_B))(R_A+H_1(ID_A,R_A)P_{pub}))\\&=H_3(h_2x_AX_B+r_Ar_BP+P_{pub}(H_1(ID_B,R_B)r_A+H_1(ID_A,R_A)r_B+sP_{pub}H_1(ID_A,R_A)H_1(ID_B,R_B))\end{aligned}$$

可得，$V_A=V_B$。签密者 A 计算得到密文 $c=V_A\oplus m$，签密接收者恢复明文 $m=V_B\oplus c$，由于 $V_A=V_B$，则确保用户能够得到正确的明文。

因为

$$\begin{aligned}T'&=uP-X_Ah_1-R_Ah_2-P_{pub}h_1'h_2\\&=(t+x_Ah_1+D_Ah_2)P-X_Ah_1-R_Ah_2-P_{pub}h_1'h_2\end{aligned}$$

$$=[T+x_A h_1 P+r_A h_2 P+sH_1(ID_A,R_A)h_2 P]-X_A h_1-R_A h_2-P_{pub} h_1' h_2$$
$$=T$$

所以

$$h_2'=H_2(m',T',R_A,X_A,R_B,X_B)=h_2$$

则能保证解密获得的消息 m 能够通过验证。

3.3 改进方案的安全性分析

1）机密性

若攻击者想从密文 $\sigma=(c,h_2,u)$ 中获得明文，就一定要计算加密密钥 V_A。若想知道获得 V_A 则须知道签密者发送者 A 的私钥。已知在第二类攻击者 A_2 的攻击下，恶意的 KGC 拥有部分私钥 D_A，若想从 X_A 中求出另一部分私钥 x_A，则面临解离散对数问题，因此加密密钥的获得是困难的，从而无法恢复出密文。其次，由于 $V_A=V_B$，若能计算出 V_B 同样可以恢复密文。但是若想求出 V_B，前提是必须计算出签密接收者 B 的全部私钥，同样面临解离散对数问题。

2）不可伪造性

改进的方案在适应性选择消息攻击下具有抗存在伪造性，针对本文对文献[1]提出的 3 种攻击方案都不能伪造出一个有效的签名。假设用户 A 为签密者，用户 B 为攻击者，B 作为签密接收者曾经与 A 完成过一次正常的签密过程，获得一个关于消息 m 的有效签密 $\sigma=(c,h_2,u)$。

a）针对攻击 1 和攻击 2，首先由于改进的方案中将公开参数 T 与加密密钥 V_A 进行绑定，使得每次的密钥都会不同。其次在改进的方案中将当前的签密消息 m 与哈希函数 H_1 进行绑定，使得建立了 u 与 h_1 之间的联系。因而，即使 B 知道 A 的部分密钥 D_A，但不知道用户自己选择的秘密值 x_A；或是 B 知道系统主密钥 s，但不知道用户自己选择的秘密值 x_A，都不能伪造出一个有效的签密。

b）针对攻击 3，通过 h_2 将签密发送者和接收者的信息进行了绑定，因此，即使存在这样一个与用户 B 进行合谋的攻击者 C，并且 B 知道用户自己选择的秘密值 x_A，但不知道 A 的部分密钥 D_A，C 也不能利用用户 B 的签密密文进行签密的伪造。

4 结语

陈虹等[11]提出一种无证书的签密方案，并在随机预言机下证明其满足机密性和不可伪造性。本文在陈虹等[11]的安全模型下，通过构造 3 种攻击方法来说明其方案不能抵抗第 1 类攻击者、第 2 类攻击者和合谋攻击，并针对这些问题，提出一种改进的无证书签密方案，同时在陈虹等[11]文献的基础上分析了方案的安全性。

参考文献：

[1] ZHENG Y L. Digital signcryption or how to achieve cost(signature & encryption) << cost(signature)+cost(encryption)[C]//International Cryptology Conference，1997.

[2] 李发根，钟笛. 数字签密综述[J]. 信息网络安全，2011(12)：1-8.

[3] SHAMIR A. Identity-based cryptosystems and signature schemes[C]//Workshop on the theory and application of cryptographic techniques. Springer，Berlin，Heidelberg，1984：47-53.

[4] BARBOSA M，FARSHIM P. Certificateless signcryption[C]//Proceedings of the 2008 ACM symposium on Information，computer and communications security，ACM，2008：369-372.

[5] 戚明平，陈建华，何德彪. 具有前向安全性的可公开验证的签密方案[J]. 计算机应用研究，2014，31(10)：3093-3094.

[6] LAI J，MU Y，GUO F. Efficient identity-based online/offline encryption and signcryption with short ciphertext[J]. International Journal of Information Security，2017，16(3)：299-311.

[7] 张庆兰. 无证书签密方案的研究及其应用[D]. 南昌：华东交通大学，2016.

[8] SHARMILA S ，SELVI D，VIVEK S S，et al. Cryptanalysis of certificateless signcryption schemes and an efficient construction without pairing[C]// International Conference on Information Security & Cryptology，Springer-Verlag，2009.

[9] 刘文浩,许春香. 无双线性配对的无证书签密方案[J]. 软件学报,2011,22(8):1918-1926.
[10] 王翔,祁正华,黄海. 不使用双线性对的无证书签密方案[J]. 计算机技术与发展,2017,27(7):106-110.
[11] 陈虹,赵悦,肖成龙,等. 可证安全的无对运算的无证书签密方案[J]. 计算机应用研究,2019(3):1-6.
[12] 汤永利,王菲菲,闫玺玺,等. 高效可证明安全的无证书签名方案[J]. 计算机工程,2016,42(3):156-160.

Attacks and Improvements of Certificateless Signcryption Scheme

Zuo Liming[1,2], Xia Pingping[1,2], Lin Nan[3]

(1.School of Science, East China Jiaotong University, Nanchang 330013, China;
2. Institute of Systems Engineering and Cryptography, East China Jiaotong University, Nanchang 330013, China;
3. State Grid Jiangxi Electric Power Co., Ltd., Electric Power Research Institute, Nanchang 330096, China)

Abstract: In order to simplify the management of certificates and keys, improve the computation efficiency and the security of the certificateless signcryption scheme at the same time, Chen Hong, et al. proposed a certificateless signcryption scheme of verifiable security without pairing and claimed that their scheme satisfied confidentiality and unforgeability in the random oracle model. Unfortunately, by constructing three types of attacks, the study indicated that Chen Hong's et al. certificateless signcryption scheme could not resist the public-key substitute attack, the master key and partial private key exposures attack, and the collusion attack. Finally, the causes of the vulnerabilities were analyzed, and the improved scheme was proposed.

Key words: signcryption; random oracle model; elliptic curve; confidentiality; unforgeability