软件学报 ISSN 1000-9825, CODEN RUXUEW
Journal of Software,2013,24(3):618−622 [doi: 10.3724/SP.J.1001.2013.04245]

E-mail: jos@iscas.ac.cn
http://www.jos.org.cn
Tel/Fax: +86-10-62562563

无证书签密机制的安全性分析*

何德彪

(武汉大学 数学与统计学院,湖北 武汉 430072)

通讯作者: 何德彪, E-mail: hedebiao@163.com

摘 要: 为了避免复杂的双线性对运算和提高签密机制的性能,Liu 等人提出了一种不使用双线性对的无证书签密机制.同时,随机谕示模型下证明了机制是可证安全.通过给出具体的攻击算法,证明了 Liu 等人所提出的机制不能抵抗类型 1 敌手的攻击.为了抵抗这种攻击,给出了一种有效的方法.

关键词: 签密;无证书;随机谕示模型;椭圆曲线

中图法分类号: TP309 **文献标识码**: A

中文引用格式: 何德彪.无证书签密机制的安全性分析.软件学报,2013,24(3):618−622. http://www.jos.org.cn/1000-9825/4245.htm

英文引用格式: HE DB. Security analysis of a certificateless signcryption scheme. Ruanjian Xuebao/Journal of Software, 2013,24(3):618−622 (in Chinese). http://www.jos.org.cn/1000-9825/4245.htm

Security Analysis of a Certificateless Signcryption Scheme

HE De-Biao

(School of Mathematics and Statistics, Wuhan University, Wuhan 430072, China)

Corresponding author: HE De-Biao, E-mail: hedebiao@163.com

Abstract: To avoid complicated pairing operation and improve performance, Liu, *et al*. proposed a pairing-free certificateless signcryption scheme, and claims that their scheme is provably secure in a strengthened security model. Unfortunately, by giving concrete attacks, the sutdy indicates that Liu's *et al*. certificateless signcryption scheme is not secure in this strengthened security model. To solve the problem, an efficient countermeasure is also proposed.

Key words: signcryption; certificateless; random oracle model; elliptic curve

公钥密码是一种实现网络和信息安全的重要技术.传统公钥密码(public key cryptography,简称 PKC)要求可信认证中心(certification authority,简称 CA)颁发证书来绑定用户的身份和公钥.这样就带来了证书管理问题,一旦用户量剧增,证书管理问题就会极大地影响系统的性能.为了解决传统 PKC 中的证书管理问题,Shamir 提出了基于身份的公钥密码[1].在基于身份公钥密码中,用户的身份(比如学号、电子邮件等)就是用户的公钥,这样就解决了传统 PKC 中的证书管理问题.然而,基于身份的公钥密码要求一个可信的私钥生成中心(key generation center,简称 KGC)通过用户的身份生成用户的私钥.这样,基于身份的公钥密码机制就面临着私钥托管问题.为了同时解决传统 PKC 和基于身份的公钥密码存在的问题,Al-Riyami 等人[2]提出了无证书公钥密码机制.这种机制可以看作一种介于传统 PKC 和基于身份的密码之间的公钥密码.

在应用中,用户在很多时候需要同时实现签名和加密.一般情况下,我们会首先通过对消息进行签名,然后再把签名进行加密来实现这一目的.1997 年,Zheng[3]提出了密码机制——签密.签密机制可以同时实现加密和签名,极大地降低计算复杂度和传输负载.Zheng 在文献[3]中提出了一个基于离散对数(discrete logarithm

* 基金项目: 高等学校博士学科点专项科研基金(20110141120003)
收稿时间: 2011-09-07; 定稿时间: 2012-04-20

problem,简称 DLP)的签密机制,但是他并没有给出可证安全性分析.在文献[4]中,An 等人系统地研究了签密机制的性质.随后,Malone 等人[5]提出了基于身份的签密机制,同时也提出了签密机制的安全模型.

自从 Al-Riyami 等人[2]提出无证书公钥密码以来,许多无证书签密机制[6−11]先后由不同的研究者提出来.2008 年,Barbosa 等人[6]首次提出了无证书签密机制.该机制使用的是先加密后签名方式,它并不能抵抗不可伪造攻击.同年,Diego 等人[7]和 Wu 等人[8]分别提出了一种无证书签密机制.Sharmila 等人[9]指出 ,Diego 等人的机制[7]不能提供保密性和认证性,Wu 等人的机制[8]不能提供保密性.Barreto[10]首次提出了签密和解签密均不需要双线性对操作的无证书签密机制,但该机制在生成公钥时需要双线性对操作;同时,该机制也不能保证发送消息的保密性和不可否认性.2009 年,Li[11]提出了一种无证书混合签密机制,并在随机谕示模型下证明了其安全性.但由于运用了对运算和指数运算,计算开销很大.上面提到的无证书签密机制都采用了对操作,与点乘运算相比,双线性对的运算要复杂得多,运行一次双线性对操作的时间大概是椭圆曲线上点乘运算的 20 倍以上[12].因此,不用双线性对运算的无证书签密机制具有更大的效率优势.基于以上情况,Liu 等人[13]提出了无需双线性对运算的无证书签密机制.同时,Liu 等人[13]在随机谕示模型下证明了其安全性.在本文中,我们指出 Liu 等人的机制不能抵抗类型 1 攻击者的攻击.这些分析表明,他们的机制是不安全的,不能够满足现实应用的需要.为了抵抗这种攻击,我们提出了一种有效的方法.

1 预备知识

1.1 椭圆曲线

设 E 是定义在有限域 F_p 上的椭圆曲线,其方程为

$$y^2=x^3+ax+b,a,b\in F_p \tag{1}$$

其判别式为

$$\Delta=4a^3+27b^2\neq 0 \tag{2}$$

则 E 上的点和无穷远点 O 构成一个群

$$G=\{(x,y):x,y\in F_p,E(x,y)=0\}\cup\{O\} \tag{3}$$

设 $P,Q\in G,l$ 是过 P,Q 和 R 的直线(如果 $P=Q$,则 l 为切线),其中,R 是 l 和 E 的第 3 个交点.设 l'是连接 R 和无穷远点 O 的直线,则定义 l'连接 R 和 O 时与 E 的第 3 个交点为 P“+”Q.点乘定义如下:

$$tP=P+P+\ldots+P(t\ times) \tag{4}$$

设群 G 的阶为 q,则有如下假设:

- 假设 1:计算性 Diffie-Hellman 问题(computational Diffie-Hellman problem,简称 CDHP):
  对未知的 $a,b\in Z_q^*$,给定(aP,bP),计算 abP 是困难的;
- 假设 2:离散对数问题(discrete logarithm problem,简称 DLP):
- 对未知的 $a\in Z_q^*$,给定 aP,计算 a 是困难的.

1.2 签密机制

无证书签密机制有 3 个合法参与者:密钥生成中心(KGC)、签密者、接收者.无证书签密机制由 7 种算法构成:

(1) 系统参数建立算法:输入安全参数 k,KGC 返回系统公开参数 $params$、保密系统主密钥 z;

(2) 用户部分密钥生成算法:输入给定用户身份 ID_i、系统参数 $params$ 和主密钥 z,KGC 输出身份 ID_i 用户的部分私钥 D_i,并通过安全渠道返回 D_i 给用户 ID_i;

(3) 用户秘密值生成算法:输入给定用户身份 ID_i、系统参数 $params$,用户 ID_i 输出其秘密值 $x_i\in Z_q^*$ 作为其长期密钥;

(4) 用户私钥生成算法:输入给定用户身份 ID_i、系统参数 $params$、ID_i 用户的部分私钥 D_i 及其长期私钥

x_i,返回用户 ID_i 私钥 $SK_i=\{x_i,D_i\}$;

(5) 用户公钥生成算法:输入用户身份 ID_i、系统参数 *params* 用户的部分公钥 P_i 及其长期私钥 x_i,返回用户公钥 PK_i;

(6) 签密算法(signcrypt):输入 *params*、消息 m、签密者身份 ID_i 及其私钥 SK_i、接收者身份 ID_j 及其公钥 PK_j,返回密文 σ;

(7) 解密验证算法(unsigncrypt):输入 *params*、σ、签密者身份 ID_i 及其公钥 PK_i、接收者身份 ID_j 及其私钥 SK_i,如果验证通过,则用户输出明文消息 m;否则,返回出错消息,拒绝接收消息 m.

2 Liu 等人的无证书签密机制

(1) 系统参数的建立

输入安全参数 k,产生两个大素数 p,q,且 $q|p-1$.P 为椭圆曲线上的循环群 G 中任意一阶为 q 的生成元,选择安全 Hash 函数: $H_1:\{0,1\}^*\times G\to Z_q^*, H_2:\{0,1\}^*\to Z_q^*, H_3:G\to Z_q^*$,明文消息 m 为任意比特长,KGC 随机选择主密钥 $z\in Z_q^*$,计算 $P_{pub}=zP$,公开系统参数$(p,q,P_{pub},H_1,H_2,H_3)$,保密主密钥 z.

(2) 用户密钥的生成

给定用户身份 ID_i,KGC 随机选择 $r_i\in Z_q^*$,计算 $R_i=r_iP, D_i=r_i+zH_1(ID_i,R_i)$,通过安全渠道返回 D_i 给用户,并作为其部分私钥,$R_i=r_iP$ 作为用户的部分公钥.

用户随机选择秘密值 $x_i\in Z_q^*$ 作为其长期私钥,生成对应的私钥(x_i,D_i),计算 $X_i=x_iP$,生成公钥(X_i,R_i).因此,用户 A 的私钥 $SK_A=\{x_A,D_A\}$,公钥 $PK_A=\{X_A,R_A\}$.用户 B 的私钥 $SK_B=\{x_B,D_B\}$,公钥 $PK_B=\{X_B,R_B\}$.

用户可以通过计算等式 $R_i+H_1(ID_i,R_i)P_{pub}=D_iP$ 是否成立来判断 KGC 分配给自己的部分私钥是否有效.

(3) 签密过程

用户 A 随机选取 $a\in Z_q^*$,计算 $T_A=aP, h_1=H_1(ID_B,R_B), h=H_2(T_A,ID_A,m), s=a/(x_A+D_A+h)$,生成签名$(h,s)$.$V_A=a(X_B+R_B+h_1P_{pub})$,$C=H_3(V_A)\oplus m$(完成加密),发送消息$\sigma=\{h,s,C\}$给用户 B.

(4) 解密验证过程

当收到密文σ后,用户 B 执行如下操作:

计算 $h_1'=H_1(ID_A,R_A), V_B=s(x_B+D_B)(X_A+R_A+h_1'P_{pub}+hP)$,恢复消息 $m=H_3(V_B)\oplus C$.

若 $h=H_2(s(X_A+R_A+h_1'P_{pub}+hP),ID_A,m)$ 成立,则用户 B 接受消息 m.

3 Liu 等人的无证书签密机制安全性分析

在文献[17]中,Liu 等人在随机谕示模型下证明了其机制是安全的.在本节中,我们将通过具体的攻击来证明其机制不能满足类型 1 攻击下的不可伪造性.设 A1 是类型 1 的攻击者,则 A1 可以查询用户公钥或替换合法用户的公钥,但不知道系统主密钥.设用户 A 和 B 分别为发送者和接受者.A 的私钥 $SK_A=\{x_A,D_A\}$,公钥 $PK_A=\{X_A,R_A\}$.B 的私钥 $SK_B=\{x_B,D_B\}$,公钥 $PK_B=\{X_B,R_B\}$.则 A1 可以通过下述方法冒充 A 产生合法的密文:

1) A1 生成随机数 $\omega\in Z_q^*$,计算 $X_A'=\omega P-(R_A+H_1(ID_A,R_A)P_{pub})$;

2) A1 利用 X_A', R_A 替换 A 的公钥 X_A.此后,B 认为 A 的公钥为 $PK_A'=\{X_A',R_A\}$;

3) A1 生成随机数 $a\in Z_q^*$,计算 $T_A=aP, h_1=H_1(ID_B,R_B), h=H_2(T_A,ID_A,m), s=a/(\omega+h)$,生成签名$(h,s)$.$V_A=a(X_B+R_B+h_1P_{pub})$,$C=H_3(V_A)\oplus m$(完成加密),发送消息$\sigma=\{h,s,C\}$给用户 B.

定理 1. A1 通过上述方法产生的密文是合法的.

证明:我们只需证明产生的密文能够通过解密验证过程即可.

由于 A1 进行了公钥替换,因此 A 的公钥为 $PK_A=\{X_A',R_A\}$,其中, $X_A'=\omega P-(R_A+H_1(ID_A,R_A)P_{pub})$.

当收到密文σ后,用户 B 计算:

$$h_1' = H_1(ID_A, R_A) \tag{5}$$

$$\begin{aligned} V_B &= s(x_B + D_B)(X_A' + R_A + h_1' P_{pub} + hP) \\ &= s(x_B + D_B)(\omega P - (R_A + H_1(ID_A, R_A)P_{pub}) + R_A + h_1' P_{pub} + hP) \\ &= a/(\omega + h)(x_B + D_B)(\omega P + hP) \\ &= a(x_B + D_B)P = a(X_B + R_B + H_1(ID_B, R_B)P_{pub}) = V_A \end{aligned} \tag{6}$$

由公式(6),我们可以得到 $V_A=V_B$.因此,B 可以恢复消息 $m=H_3(V_B)\oplus C$.

另外,B 计算

$$\begin{aligned} H_2(s(X_A' + R_A + h_1' P_{pub} + hP), ID_A, m) &= H_2(a/(\omega + h)(\omega P - (R_A + H_1(ID_A, R_A)P_{pub}) + R_A + h_1' P_{pub} + hP), ID_A, m) \\ &= H_2(a/(\omega + h)(\omega P + hP), ID_A, m) \\ &= H_2(aP, ID_A, m) \\ &= H_2(T_A, ID_A, m). \end{aligned}$$

而 $h=H_2(T_A,ID_A,m)$,因此 $h = H_2(s(X_A' + R_A + h_1' P_{pub} + hP), ID_A, m)$ 成立,用户 B 接受消息 m.A1 成功地伪造了一组合法密文. □

从以上分析得知,接收者使用 $L_A=X_A+R_A+H_1(ID_A,R_A)P_{pub}$ 来验证密文的正确性.很显然,L_A 是 X_A 和 $R_A+H_1(ID_A,R_A)P_{pub}$ 的简单线性组合.A1 正是利用了这种线性关系通过自己可以控制的 X_A 来消除 $R_A+H_1(ID_A,R_A)P_{pub}$ 对密文的影响.为了抵抗 $A1$ 的攻击,必须要破坏这种线性关系.我们只需要对用户密钥生成算法和解密算法做如下修改即可抵抗 A1 的攻击:

(1) 用 $D_i=r_i+zH_1(ID_i,R_i,X_i)$替换用户密钥的生成中的 $D_i=r_i+zH_1(ID_i,R_i)$;

(2) 用 $h_1' = H_1(ID_A, R_A, X_A)$ 替换解密过程中的 $h_1' = H_1(ID_A, R_A)$.

经过上述改变,接收者使用 $L_A=X_A+R_A+H_1(ID_A,R_A,X_A)P_{pub}$ 验证密文的正确性.由于 H_1 是一个安全的杂凑函数,A1 不可能通过选择的 X_A 来消除 $R_A+H_1(ID_A,R_A,X_A)P_{pub}$ 的作用.因此,这种改变可以抵抗类型 1 敌手的攻击.

4 总 结

Liu 等人[13]提出了一种高效的无证书签密机制,并且在一种高强度的安全模型下证明了其安全性.在本文中,我们在 Liu 等人的安全模型下,通过构造具体的攻击方法来表明其机制不能满足类型 1 攻击下的不可伪造性.我们的分析表明,Liu 等人的签密机制不能够满足现实应用的需要.

致谢 感谢外审专家的精心评审,感谢各位编辑的辛勤劳动.

References:

[1] Shamir A. Identity-Based cryptosystem and signature scheme. In: Advances in Cryptology-Crypto'84. LNCS 196, Berlin: Springer-Verlag, 1984. 47−53. [doi: 10.1007/3-540-39568-7_5]

[2] Al-Riyami S, Paterson K. Certificateless public key cryptography. In: Laih CS, ed. Proc. of the Int'l Association for Cryptdology Research 2003. LNCS 2894, Berlin: Springer-Verlag, 2003. 452−473. [doi: 10.1007/978-3-540-40061-5_29]

[3] Zheng Y. Digital signcryption or how to achieve cost(signature & encryption)<<cost(signature)+cost(encryption). Advances in Cryptology-Crypto'97. LNCS 1294, Berlin: Springer-Verlag, 1997. 291−312. [doi: 10.1007/BFb0052234]

[4] An J, Dodis Y, Rabin T. On the security of joint signature and encryption. In: Knudsen LR, ed. Proc. of the Eurocrypt 2002. LNCS 2332, Berlin: Springer-Verlag, 2002. 83−107. [doi: 10.1007/3-540-46035-7_6]

[5] Malone-Lee J. Identity based signcryption. Report, 2002/098, 2002. http://eprint.iacr.org/2002/098

[6] Barbosa M, Farshim P. Certificateless signcryption. In: Proc. of the ACM Symp. on Information, Computer and Communications Security (ASIACCS 2008). ACM Press, 2008. 369−372. [doi: 10.1145/1368310.1368364]

[7] Aranha D, Castro R, Lopez J, Dahab R. Efficient certificateless signcryption. 2008. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_01_resumo.pdf

[8] Wu CH, Chen ZX. A new efficient certificateless signcryption scheme. In: Proc. of the ISISE 2008. 2008. 661−664. [doi: 10.1109/ISISE.2008.206]

[9] Sharmila DS, Vivek SS, Pandu RC. On the security of certificateless signcryption schemes. Report, 2009/298, 2009. http://eprint.iacr.org/2009/298

[10] Silva RR. Toward efficient certificateless signcryption from (and without) bilinear pairings. 2008. http://sbseg2008.inf.ufrgs.br/proceedings/data/pdf/st03_03_artigo.pdf

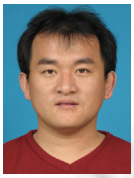
[11] Li FG, Shirase M, Takagi T. Certificateless hybrid signcryption. In: Proc. of the ISPEC 2009. LNCS 5451, Berlin, Heidelberg: Springer-Verlag, 2009. 112−123. [doi: 10.1007/978-3-642-00843-6_11]

[12] Chen L, Cheng Z, Smart NP. Identity-Based key agreement protocols from pairings. Int'l Journal of Information Security, 2007, 6(4):213−241. [doi: 10.1007/s10207-006-0011-9]

[13] Liu W, Xu C, Certificateless signcryption scheme without bilinear pairing. Ruanjian Xuebao/Journal of Software, 2011,22(8): 1918−1926 (in Chinese with English abstract). http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001. 2011.03891]

附中文参考文献:

[13] 刘文浩,许春香.无双线性配对的无证书签密机制.软件学报,2011,22(8):1918−1926. http://www.jos.org.cn/1000-9825/3891.htm [doi: 10.3724/SP.J.1001.2011.03891]



何德彪(1980－),男,山东阳谷,博士,讲师,
主要研究领域为密码学,信息安全.
E-mail: hedebiao@163.com