第32卷 第23期 计 算 机 工 程 2006年12月
Vol.32 No.23 Computer Engineering December 2006
·安全技术· 文章编号：1000—3428(2006)23—0153—03 文献标识码：A 中图分类号：TN918.1

基于Brier-Joye的Elgamal椭圆曲线密码体制研究

李宗秀，鲍皖苏，汪 翔
（解放军信息工程大学电子技术学院，郑州 450004）

摘 要：对二元域上基于 Brier-Joye 公式的 Elgamal 椭圆曲线密码体制的安全性进行了分析，给出了抵抗碰撞点攻击的方法，介绍了 Brier-Joye 公式抵抗信道攻击的椭圆曲线选择标准。

关键词：侧信道攻击；碰撞点；异常点；Elgamal 型椭圆曲线密码；Brier-Joye 公式

Research on Elgamal-elliptic Curve Cryptosystem Based on Brier-Joye Formula

LI Zongxiu, BAO Wansu, WANG Xiang
(Institute of Electronic Technology, PLA Information Engineering University, Zhengzhou 450004)

【Abstract】 This paper analyzes the security of Elgamal elliptic curve cryptosystem with Brier-Joye formula on binary fields, proposes some countermeasures to collision-point attack and gives standards of choosing elliptic curves to resist side channel attack, which make the Brier-Joye formula work well.

【Key words】 Side channel attack; Collision point; Exceptional point; Elgamal elliptic curve cryptosystem; Brier-Joye formula.

椭圆曲线公钥密码体制现在是公钥密码学的研究热点，与传统的 RSA 公钥算法相比，其具有密钥短、速度快、存储和带宽要求低、安全性高等优点。因其明显的优越性，人们对 ECC 进行了很多研究，其中对 ECC 的安全性研究是 ECC 研究中非常重要的内容。由于 ECC 的运算特点，出现了一种比较新的对 ECC 很有效的攻击。这就是 Kocher P 在 1996 年提出时对 ECC 的窃听信道攻击(Side channel attack, SCA)，这种分析假定攻击者能够得到信道的相关信息，例如运行时间的差异、脉冲的不同或者电功率消耗的差异，攻击者得到这些信息后，根据椭圆曲线群算法规则中的点加和倍乘公式，从而导致脱密时信道的电功率消耗因密钥 bit 的变化而不同，就可以推断出私钥的若干比特信息。这种新的攻击方法迫使研究者要考虑椭圆曲线群的基础运算的新方法。于是 Brier 和 Joye 提出了新的标准 Weierstrass 椭圆曲线群上的点运算公式(B-J 公式)，使得点加和倍乘 2 种运算都可以用同一个公式进行计算，这样就可以有效地抵抗 SCA。但是文献[1]在 2002 年提出了对素域上使用 B-J 公式的 ECC 的攻击，这种攻击是基于使用 B-J 公式的 Elgamal 椭圆曲线密码体制的特定的加脱密标准而提出的。本文对二元域上的 Elgamal 椭圆曲线密码体制的 B-J 的应用进行了研究，发现这种攻击同样适用于二元域。

1 预备知识

在研究开始之前，给出以下表述和定义，且这些定义适用于全文。

对椭圆曲线上的一点 $P=(x,y)$，$x(P)$ 表示点 P 的 x 坐标，$y(P)$ 表示点 P 的 y 坐标。特别地，在点 P 的射影坐标系统下，$Z(P)$ 表示点 P 的 Z 坐标。

定义 1 设 P_1 和 P_2 是椭圆曲线上的两个点，如果有 $x(P_1)\neq x(P_2)$ 且 $y(P_1)=y(P_2)$，则称 P_1、P_2 满足 DZ 条件。

定义 2 设 P_1 和 P_2 是椭圆曲线上的两个点，如果 P_1、P_2 满足 DZ 条件，则称 (P_1,P_2) 是一个碰撞对。如果 (P_1,dP_1) 是一个碰撞对，则称 P_1 是 d 次自碰撞点。

为了后面的分析，下面给出 Elgamal 椭圆曲线密码体制的具体实施方案。令 u 是私钥，Q 是公钥，$Q=uP$，消息 M 是 E 上的一点。

有关加密方(Alice)的描述如下：(1)计算 $C_1=rP$，对任意选取的随机整数 $r(o\le r<n)$；(2)计算 $C_2=M+rQ$；(3)发送密文 $C=(C_1,C_2)$ 给 Bob。

有关脱密方(Bob)的描述如下：(1)计算 $R=uC_1$；(2)得到明文 $M'=C_2-R$。

2 碰撞点攻击

2.1 窃听信道攻击和 B-J 公式

窃听信道攻击是假定攻击者可以得到密钥持有者进行脱密时的信道信息，例如时间的差异、脉冲的不同、能量的消耗差异等。攻击者得到这些信息以后经过分析就可以得到密钥的若干信息。这一攻击的主要理论依据是：椭圆曲线群的点加和倍乘运算要用不同的公式，这就使得点加和倍乘运算的电功率消耗明显不同，即信道信息的变化依赖于密钥比特

基金项目：河南省杰出青年科学基金资助项目(0312001800)
作者简介：李宗秀(1978－)，女，硕士，主研方向：密码学；鲍皖苏，教授；汪 翔，博士生
收稿日期：2006-03-01 **E-mail：**xiu1496@163.com

的变化，泄漏了密钥的比特信息[2]。这是因为在解密时，计算kP时常用到下列算法(Double and add))：

$Input: P, k = (1, k_{l-2}, ..., k_0)_2$

$Onput: Q = kP$

$R_0 \leftarrow P$

$for\ \ j = l-2\ down to\ 0\ do$

$\quad R_0 \leftarrow 2R_0$

$\quad if\ (k_j = 1)\ then\ R_0 \leftarrow R_0 + P$

$end\ for$

$return\ R_0$

由于椭圆曲线点加和倍乘所用的公式不同，因此在运算时，能量消耗也明显不同，这时通过探测信道的能量消耗，就可以判定参与运算的密钥比特是 0 或是 1。

对于由于使用 Double-and-add 算法而引发的信道攻击，文献[2，4]给出了抵抗方法，即使用 Coron 的点加、倍乘算法，或者使用 Montgomery 标量乘算法，这 2 种算法相对都比较费时。

Brier 和 *Joye* 提出了椭圆曲线群上非标准的加法公式，即 B-J 公式，来针对由于椭圆曲线的点加和倍乘所用公式不同而引发的信道攻击，此公式使得 $Double-and-add$ 算法可以安全使用。

对于特征大于3的有限域 $F_q(q=p^m)$ 上的标准Weierstrass椭圆曲线 $E: y^2 = x^3 + ax + b$ 上的两点 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$，其中 $y_1 \neq -y_2$，则 $P_3 = (x_3, y_3) = P_1 + P_2$ 的坐标由下式给出：

$$x_3 = \lambda^2 - x_1 - x_2, \quad y_3 = -\lambda x_3 - \mu$$

其中

$$(\lambda, \mu) = \left(\frac{x_1^2 + x_1 x_2 + x_2^2 + a}{y_1 + y_2}, y_1 - \lambda x_1 \right)$$

Brier 和 Joye 还提出了在投影坐标下计算 $P_1 + P_2$ 的有效算法：令 $P_1 = (X_1 : Y_1 : Z_1)$ 和 $P_2 = (X_2 : Y_2 : Z_2)$ 为椭圆曲线上的点，则 $P_3 = (X_3 : Y_3 : Z_3) = P_1 + P_2$ 由下式给出

$$X_3 = 2FW, \ \ Y_3 = R(G - 2W), \ \ Z_3 = 2F^3$$

其中，共用 18 次域中乘法。

$$U_1 = X_1 Z_2, \ U_2 = X_2 Z_1, \ T = U_1 + U_2, \ R = T^2 - U_1 U_2 + a(Z_1 Z_2)^2,$$
$$M = Y_1 Z_2 + Y_2 Z_1, \ F = Z_1 Z_2 M, \quad L = MF, \ G = TL, \ W = R^2 - G$$

Brier 和 Joye 还给出了有限域 F_2^m (m 是素数)上的统一公式：有限域 F_2^m (m 是素数)上非超奇异椭圆曲线为

$$y^2 + xy = x^3 + ax^2 + b$$

其中，$b \neq 0$ 时 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$，$y(P_1) \neq y(-P_2)$，则

$$x_3 = \lambda^2 + \lambda + x_1 + x_2 + a, \qquad y_3 = (\lambda + 1)x_3 + \mu$$

$$(\lambda, \mu) = \left(\frac{x_1^2 + x_1 x_2 + x_2^2 + a x_1 + a x_2 + y_1}{y_1 + y_2 + x_2}, y_1 - \lambda x_1 \right)$$

从 B-J 公式可以看出，对椭圆曲线上的点加和倍乘可以用相同的公式去计算，不管密钥比特是 0 或 1 都进行相同的运算过程，这样就有效地抗击了 SCA。

但是对于使用 B-J 公式 Elgamal 椭圆曲线密码体制，文献[1]却给出了针对使用 B-J 公式的碰撞点攻击，这种攻击即使在密码算法计算中的标量乘使用 Coron 的点加、倍乘算法，或者使用 Montgomery 标量乘算法时，仍然有效，这就促使研究者在使用新的公式时要仔细考虑算法的安全性。

2.2 对 Elgamal 椭圆曲线密码体制的碰撞点攻击

文献[1]中的对 B-J 公式的碰撞点攻击是对素域上 Weierstrass 椭圆曲线而言的。对于椭圆曲线上的两点 P_1、P_2，如果满足 $P_1 + P_2 = 0$，那么就有 $y(P_1) = y(-P_2)$，反之，若 $y(P_1) = y(-P_2)$, $P_1 + P_2$ 不一定等于 0，就是说在计算 uP 时，可能计算到 $P_1 + P_2$ 满足 $y(P_1) = y(-P_2)$ 且 $x(P_1) \neq x(P_2)$，这就给碰撞点攻击提供了可能。为了避免最为费时的求逆运算，在计算标量乘时通常利用射影坐标系统，在计算 $P_1 + P_2$ 时，若满足 $y(P_1) = y(-P_2)$。

由B-J公式的射影坐标公式可以看出，这等价于 $Y_1 Z_2 + Y_2 Z_1 = 0$，因为 $Z_3 = 2Z_1^3 Z_2^3 (Z_1 Z_2 (Y_1 Z_2 + Y_2 Z_1))^3$，所以 P_3 的 Z 坐标 $Z_3 = 0$，一旦出现 Z 坐标为零的点作为下一循环的输入，此步以后的 Z 坐标均为 0，这样就得到 $Z_u = 0$，在标量乘的最后要把射影坐标转化为仿射坐标，即通过$x_u=X_u/Z_u$、$y_u=Y_u/Z_u$把 $up = (X_u : Y_u : Z_u)$ 转化为

$$up = (x_u, y_u)$$

因为 $Z_u = 0$，这就导致仿射坐标下求逆是不存在的，从而出现错误，得不到正确的结果。攻击者正是利用这个错误，窃听到信道中出错信息，找出导致出错的 P_1 与 P_2 的倍数关系，就可以得到相应的密钥 bit 信息。然而，找出 P_1 与 P_2 的关系，这无异于解离散对数问题，攻击效果不佳。

攻击者利用B-J公式的异常点及Elgamal椭圆曲线密码体制的特点进行攻击，把选择密文攻击和窃听信道攻击相结合，就能得到想要的密钥bit信息。Elgamal椭圆曲线密码体制中，因为发方发出的 C_1 是任意的，所以攻击者把事先准备好的X发给收方，收方并不会发觉。假若Elgamal椭圆曲线密码体制算法中收方Bob脱密时的算法[2](Coron的点加、倍乘算法)如下：

$Input: P, u = (1, u_{k-2}, u_{k-3}, ..., u_0)_2$

$Output: Q = uP$

$\quad R_0 \leftarrow P$

$for\ \ j = k-2\ down\ to\ 0\ do$

$R_0 \leftarrow 2R_0; \quad R_1 \leftarrow R_0 + P$

$b \leftarrow u_j; \quad R_0 \leftarrow R_b$

$End\ \ for$

$return\ R_0$

以下给出其攻击原理：攻击者要猜测 u_{k-2} 时，首先生成一个 2 次自碰撞点 X，即：$R_1 = 2X + X$ 的射影坐标的 Z 坐标为 0，当 X 发给上述 Elgamal 椭圆曲线密码体制算法中脱密者 Bob 时，Bob 用 Coron 的算法进行脱密。若猜测 $u_{k-2} = 1$ 正确，则此圈循环输出 $R_0 = R_1 = 2X + X$ (且 $Z(R_0) = 0$)作为下一圈循环的输入，由上面的分析可得以后输出的 R_0 的 Z 坐标均为 0 ，这就导致最后输出出错信息。否则，若没有出现错误，说明此圈输出 $R_0 = 2X$ ，则 $u_{k-2} = 0$。猜测 u_{k-3} 时方法相同，若 $u_{k-2} = 1$ 时，生成一个 6 次自碰撞点 X'，否则生成一个 4 次自碰撞点。

攻击者得到 u_{k-2} 和 u_{k-3} 后，就可以用相同的方法不断重发事先准备好的相应 X，使收方进行多次脱密，这样攻击者就能得到相继的 $u_{k-4}, u_{k-5}, u_{k-6}, \ldots$。

但是为了从 $u_{k-2}, u_{k-3}, \ldots, u_{i+1}$ 猜出 $u_i (i = 1, 2, 3, \ldots)$，攻击者就不得不事先选取一个点 $X \in E$，使得 X 与

$2(...,2(2(2X+u_{k-2}X)+u_{k-3}X)+,...,+u_{i+2}X)+u_{i+1}X$ 满足 DZ 条件。事先找到一些自碰撞点并不容易，而且这些自碰撞点的次数应是唯一的。文献[1]给出了找自碰撞点的方法，并给出了 $2 \le d \le 9$ 的一些适合密码用的椭圆曲线上的自碰撞点的个数。对较大的 d，目前没有有效算法来寻找自碰撞点。

3 碰撞点攻击分析

3.1 Elgamal 椭圆曲线密码体制的安全性

以上对素域上基于 B-J 公式的 Elgamal 椭圆曲线密码体制的安全性进行了分析，对于 F_2^m 上基于 B-J 公式的 Elgamal 椭圆曲线密码体制，同样存在由于使用 B-J 公式而引发的安全性问题。下面对 F_2^m 上的椭圆曲线的 B-J 公式进行了研究，给出了其射影坐标的有效算法。

F_2^m 上的非奇异椭圆曲线形式为

$y^2+xy=x^3+ax^2+b,(b\neq 0)$

E 上的射影坐标点 $(X:Y:Z)$ 对应的仿射坐标为 (X/Z,Y/Z)，射影方程为

$$Y^2Z+XYZ=X^3+aX^2Z+bZ^3 \tag{1}$$

令 $P_1=(X_1:Y_1:Z_1),\ P_2=(X_2:Y_2:Z_2)$ 是式(1)上的两点，下面给出 B-J 公式下的 $P_3=(X_3:Y_3:Z_3)=P_1+P_2$ 的坐标表示为

$$X_3=B^2+AB+WD,\qquad Y_3=B^2+WD(A+B)+FG,Z_3=A^3$$

其中，$A_1=Y_1Z_2+Y_2Z_1,A_2=Y_1Z_2,B_1=Z_2X_1+Z_1X_2,C=X_1X_2Z_1Z_2,$

$U_1=Z_1Z_2,U_2=A_1+Z_1X_2,G_1=Y_1U_2,G_2=X_2B,B=B_1^2+C+U_1(aB_1+A_2),$

$A=U_1U_2,\qquad D=AU_2,E=A^2U_1Z_2,\qquad F=G_1+G_2,W=B_1+aU_1,$

$Z_3=Z_1^3Z_2^3(Y_1Z_2+(Y_2+X_2)Z_1)^3,$

定义这里的异常点为：满足 $y(P_1)=y(-P_2)$ 且 $x(P_1)\neq x(P_2)$ 的点，这样，若 P_1 和 P_2 为 F_2^m 上的椭圆曲线的异常点，仍然有 $Z_3=0$，上述攻击对 F_2^m 上的椭圆曲线 B-J 公式同样有效。由此可以看出，文献[1]中攻击方法的实施依赖于椭圆曲线群基础运算公式的形式，以及碰撞点的存在性和椭圆曲线密码特定加脱密方案的特点。要抵抗这一攻击，又要保证 B-J 公式的使用，就要从密码体制本身的加脱密标准和 B-J 公式的碰撞点 2 个方面进行改进。

3.2 抵抗碰撞点攻击

从 Elgamal 椭圆曲线密码体制的实施方案和 B-J 公式的碰撞点 2 个方面进行研究，给出以下抵抗上述碰撞点攻击的方法。

(1)收方收到消息 C' 后，无论消息是真是假，它都随机挑选曲线上一点 R，然后计算 $u(C'+R)-uR$。假如收方收到攻击者发给他的消息 (X,C_2)，就先随机生成椭圆曲线上一点 R，然后计算 $u(X+R)-uR$，这样就打乱了攻击者利用 X 是 d 次自碰撞点的攻击企图。以上算法中一个重要的问题就是 R 的选取。首先 $R\neq -X$，其次如果 X 是 d 次自碰撞点，R 不能是 d 次自碰撞点，若是，计算标量乘 $u(X+R)$ 时，若计算到 $d(X+R)+(X+R)=dX+dR+X+R$ 作为输出时，仍会出现攻击者预期的错误信息，并且由这一信息能得到正确的密钥比特信息。由文献[1]可知，当 d 比较大时，求 d 次自碰撞点对问题目前没有有效算法，不妨假定收到的 X 是 d 次自碰撞点 $(2\le d\le 10)$，在选择随机点时，先计算 $2R,3R,4R,\ldots,9R,10R$，然后验证 R 是否是 d 次自碰撞点，若 R 与 $dR(2\le d\le 10)$ 满足 DZ 条件，则抛弃再次选择。这样选择的 R 就能降低攻击的成功率。

(2)随机化密钥 u，即收到 C' 后，计算 $(u+rn)C'$。其中，r 是随机数，n 是椭圆曲线的阶。在这种情况下，攻击者仍能够得到错误的密钥信息，即 $(u+rn)$ 的比特信息，由于 r 是随机数，因此得不到正确的密钥信息。

3.3 选择安全的椭圆曲线参数

由于一个椭圆曲线群上的自碰撞点的寻找不仅与标量 u 的加法链有关，还与椭圆曲线各个参数(基点的阶 P 和系数 a,b)有关。若在椭圆曲线群计算的参数选取上使攻击者找到自碰撞点不可行，这一攻击就会不复存在，要根本避免这一攻击，这种方法是最彻底的。这里有 2 层涵义：(1)定义的椭圆曲线群上不存在碰撞点；(2)对任意选择的点 X 都没有低阶自碰撞点，这样就使攻击者在计算能力范围内找不到合适的自碰撞点。下面对这一问题进行了探讨。

要使B-J公式能够很好应用，就必须在选择基点P时充分考虑P的自碰撞点情况，最好的情况是P不是 $d\ (2\le d\le u-1)$ 次自碰撞点。对一条给定的椭圆曲线(标准Weierstrass曲线)，选择基点P时，既要考虑P的阶：P的阶要足够大；又要考虑P的自碰撞点。对素域上的情况，若要使选定的椭圆曲线上任何一点 $P=(x_1,y_1)$ 无自碰撞点，就要使式(2)在 F_P 上无异于 x_1 的解[1]。

$$x^2+st+t=0 \tag{2}$$

其中，$x^3+ax+b-y_1^2=(x-x_1)(x^2+sx+t)$。

式(2)若有异于 x_1 的解 x_2，则有

$x_2^3+ax_2+b-y_1^2=(x_2-x_1)(x_2^2+sx_2+t)=0$

即 $x_2^3+ax_2+b=y_2^2=y_1^2$，进而可得 $y_2^2=y_1^2$，若 $y_1\neq y_2$，那么 $y_1=-y_2$，这意味着 $P=(x_1,y_1)$ 有碰撞点。把判定 $P=(x_1,y_1)$ 有无碰撞点问题转化为式(2)在 F_p 上有无异于 x_1 的解的问题。由 (Konig-Rados)定理，要使式(2)在F_p上无解，需使下列矩阵满秩：

$$\begin{pmatrix} t & s & 1 & \cdots & 0 & 0 & 0 \\ s & 1 & 0 & \cdots & 0 & 0 & t \\ 1 & 0 & 0 & \cdots & 0 & t & s \\ 0 & 0 & 0 & \cdots & t & s & 1 \\ \vdots & \vdots & \vdots & \cdots & \vdots & \vdots & \vdots \\ 0 & 0 & t & \cdots & 0 & 0 & 0 \\ 0 & t & s & \cdots & 0 & 0 & 0 \end{pmatrix} \tag{3}$$

上述矩阵为 $(p-1)\times(p-1)$ 的方阵。由于 $x^3+ax+b-y_1^2=(x-x_1)(x^2+sx+t)$，可得 $s=x_1,t=x_1^2+a$，由于 $t\neq 0$，a 是 F_P 上的非平方剩余。为使选择的椭圆曲线任意一点 $P=(x_1,y_1)$ 均无碰撞点，就要满足如下 2 个条件：(1)式(3)满秩；(2)a 是 F_P 上的非平方剩余。

要使B-J公式顺利应用、使碰撞点攻击不能奏效，在选择椭圆曲线及基点时就要遵循上述标准。至于使选定的椭圆曲线群上的点不存在低阶自碰撞点，这就要计算所有的低阶多项式，使相应的碰撞多项式[1]在椭圆曲线基域上无解。

4 结论

用统一公式取代传统椭圆曲线群上的加法公式，来抵抗 SCA，它虽然能够掩盖由于计算公式不同而引发的信息泄漏，但是公式本身的特点引发了新的攻击，这种攻击对密钥的威

（下转第 173 页）