同源密码中 Montgomery 模型的 *w*-坐标研究

陶 铮[1], 胡 志[1]

[1] 中南大学数学与统计学院 长沙 中国 410083

摘要 椭圆曲线群律计算是传统椭圆曲线密码(ECC)的核心运算, 同时也是基于同源的后量子密码计算中的重要组成部分。Montgomery 曲线上的 Montgomery ladder 算法是一种高效(伪)群律计算方法, 且经常用于预防侧信道攻击。 Farashahi 和 Hosseini 在 ACISP 2017 提出了 Edwards 曲线模型上的 *w*-坐标可得到类似 Montgomery ladder 算法以进行群律计算, Kim 等人在 ASIACRYPT 2019 将其用于优化奇数次同源计算。随后, 不同曲线模型上的 *w*-坐标陆续被提出用于优化同源计算。本质上, *w*-坐标是关于传统椭圆曲线有理点(*x*, *y*)-坐标的有理函数。与标准 (*x*, *y*)-坐标相比, *w*-坐标不仅可以节约椭圆曲线群律和同源计算的计算量, 还可以减少带宽。Hisil 和 Renes 在 ACM TOMS 2019 提出可利用加 2 阶点得到更多的 *w*-坐标。受此启发, 本文提出利用 Montgomery 曲线上的 2-同源构造出 3 类新的 *w*-坐标, 与 *x*-坐标相同的是, 均可应用于 Montgomery ladder 算法和奇数次同源计算的优化。同时, *w*-坐标在计算奇数次同源中, 同源映射像曲线系数计算公式与像点公式类似, 可利用 SIMD 指令集将两者并行化处理, 从而得到相关计算的进一步加速。最后, 由于 Edwards, Huff, Jacobi 等曲线模型在某些条件下可与 Montgomery 模型建立双有理等价, 因此可由 Montgomery 曲线上新的 *w*-坐标开发出其他曲线模型上更多的 *w*-坐标, 它们将有可能支持同源密码实现中更有效的算法。

关键词 后量子密码; 同源; Montgomery 曲线; *w*-坐标

中图法分类号 TP 309.7 DOI 号 10.19363/J.cnki.cn10-1380/tn.2021.11.08

On the *w*-coordinates of Montgomery Model in Isogeny-based Cryptography

TAO Zheng[1], HU Zhi[1]

[1] School of Mathematics and Statistics, Central South University, Changsha 410083, China

Abstract Elliptic curve group law calculation is the core operation of traditional Elliptic Curve Cryptography (ECC), which is also an important part of isogeny-based post quantum cryptography. The Montgomery ladder algorithm on Montgomery curve is an efficient (pseudo) group law calculation method, which is commonly used to resist side channel attacks. Farashahi and Hosseini in ACISP 2017 proposed the *w*-coordinates on Edwards curve model which could induce Montgomery-like ladder algorithm for group law calculation. By adopting such w-coordinates, Kim et al. in Asiacrypt 2019 optimized odd order isogeny computation. After that, several works have been devoted to extensively exploiting *w*-coordinates on different elliptic curve models. Essentially, the *w*-coordinates are rational functions of the traditional (*x, y*)-coordinates for rational points. Compared with the standard elliptic curve rational point (*x, y*)-coordinate, the *w*-coordinate not only reduces the amount of intermediate calculation in group law calculation and isogeny calculation, but also saves half of the bandwidth. Hisil and Renes in ACM TOMS 2019 considered how to obtain more *w*-coordinates by adding some 2-torsion point. Inspired by their work, this paper proposes three new *w*-coordinates by using a 2-isogeny on Montgomery curve, which are similar to the *x*-coordinate. These *w*-coordinates can be applied to Montgomery ladder algorithm, as well as to the optimization of odd degree isogeny computation. Simultaneously, in the calculation of the odd-numbered homology of the *w*-coordinate, the calculation formula of the Montgomery curve coefficient is similar to the isogeny formula, so the SIMD instruction set can be used to parallelize the coordinate calculation and the coefficient calculation, so as to obtain the further acceleration of the isogeny calculation. Moreover, since curve models such as Edwards, Huff, and Jacobi can establish a rational equivalent mapping with the Montgomery curve model under certain conditions, more *w*-coordinates can be developed from the three new types of *w*-coordinates, which implies such curve models can possess more *w*-coordinates to design better algorithms for isogeny based cryptography.

Key words post-quantum cryptography; isogeny; Montgomery curve; *w*-coordinate

通讯作者: 胡志, 博士, 副教授, Email: huzhi_math@csu.edu.cn.

本课题得到国家自然科学基金（No. 61972420, No. 61602526）和湖南省自然科学基金（No. 2020JJ3050, No.2019JJ50827）资助.

收稿日期: 2021-08-30; 修改日期: 2021-10-12; 定稿日期: 2021-10-20

1 引言

近年来随着量子计算机研究的飞速发展, 以 Shor 算法[1]为典型代表的量子算法的具体实现迎来了曙光, 这也预示着目前正使用的公钥密码系统(如 RSA 和 ECC)将不再安全, 由此将严重危害网络空间中数字通信的机密性和完整性。基于一些在量子计算模型下目前仍是计算困难的问题, 许多新的公钥密码方案被提出, 包括基于格的密码, 基于编码的密码, 基于 Hash 的密码, 基于多变量多项式的密码, 以及基于超奇异椭圆曲线上同源计算的密码, 等。公钥密码的研究由此进入了后量子时代。

1.1 基于同源的后量子密码

基于超奇异椭圆曲线同源计算的公钥密码体制由 Jao 和 De Feo 在 2011 年提出[2], 其安全性依赖于寻找两条定义在有限域 F_q 上超奇异椭圆曲线间同源映射的复杂性。目前该问题在量子计算模型下仍是指数时间复杂度的。在美国国家标准与技术研究院(National Institute of Standards and Technology, NIST)启动的后量子密码学标准化计划中, 基于同源的密码方案——超奇异同源密钥封装(Supersingular Isogeny Key Encapsulation,SIKE) 在三轮角逐中均进入公钥加密与密钥建立方案的候选列表[3]。

相对于其他后量子密码, 基于超奇异椭圆曲线同源计算的密码主要有两大优势: (1)由于椭圆曲线具有良好的代数结构, 在相同安全级别条件下, 基于同源的密码具有相对较小的密钥长度; (2)传统 ECC 已有三十多年的研究历史, 关于 ECC 的快速实现和安全防护技术的研究日趋成熟, 故而对于密码系统使用者和实现者而言, 基于同源的密码系统可以更为方便的在未来部署和保护。然而, 同源计算相比 ECC 中的标量乘法运算而言要复杂得多, 与其他后量子密码相比, 同源密码的实现效率不占优势, 这也极大地影响了其走向实际应用。

1.2 同源密码实现与 w-坐标

许多密码学者研究基于超奇异同源密码的高效安全实现, 其中主要运算包括有限域算术、椭圆曲线群律以及同源映射等。有限域算术作为最底层运算适合硬件优化实现[4], 而后两者运算尤其是同源运算较为复杂, 因此优化同源以及群律计算, 是我们所关注的重点[5]。目前超奇异同源密码实现中主要采用 Montgomery 曲线模型, 因其可用 Montgomery ladder 算法高效安全实现椭圆曲线群律运算[6], 已有关于同源计算的优化工作以及硬件实现也主要集中在该类曲线模型上[7]。

一般的, 椭圆曲线 E 作为射影直线 P 的 2 覆盖, 可诱导从 $E/\{\pm 1\}$ 到 P 的同构映射, 并由此引出 P 上的(伪)群律(此时该射影直线称为 Kummer 线)。对于 Montgomery 曲线而言, x-坐标诱导了从 $E/\{\pm 1\}$ 到 P 的同构映射, 因此椭圆曲线算术可以只用 x-坐标进行, 在简化运算的同时还可以节省带宽。Karati 和 Sarkar 还提出了平方化的 Kummer 线, 并指出其算术可通过单指令多数据流(Single Instruction Multiple Data, SIMD)指令集加速计算[8]。Hisil 和 Renes 还证明了可以通过加 2 阶点的方式所构造的同构映射得到新的 Kummer 线[9]。

实际上, 在许多应用场景我们并不需要上述诱导映射为同构映射, 从而可考虑一种 Kummer 线上 x-坐标的推广形式— $w-$ 坐标(关于椭圆曲线上有理点坐标的一个有理函数), 来完成椭圆曲线上的群律计算与同源映射计算。自然的, Montgomery 曲线模型上的 x-坐标可视为 w-坐标的一个特例, 目前已广泛应用于椭圆曲线群律计算和同源计算。Farashahi 和 Joye 针对特征为 2 的有限域上的 Hessian 曲线模型给出了 w-坐标满足差分加法运算[10]; Farashahi 和 Hosseini 提出了 Edwards 曲线模型上的 w-坐标[11], 其诱导产生的差分加法同样适配 Montogomery ladder 算法。Kim 等人[12]随后将该 w-坐标技术用到了同源计算中, 得到了目前关于一些小的奇数阶同源的最好计算结果。Huang 等人[13]和 Drylo 等人[14]各自独立提出 Huff 曲线模型上的 w-坐标用于高效群律计算和同源计算。

使用 w-坐标来实现椭圆曲线群律计算和同源计算的优点主要有:

(1) w-坐标支持点的差分加法运算(即已知点 P, Q, P-Q, 可计算点 P+Q), 加法和倍点计算运算效率高。设 M, S, a 分别表示有限域中的乘法、平方和加法运算。以 Montgomery 曲线模型为例, 其差分加法/倍点运算仅需 4M+2S (若令 Z-坐标为 1, 则计算代价还可以减少 1M)。

(2) w-坐标的差分加法运算可适配 Montgomery ladder 算法, 标量乘法计算的每轮迭代计算量一致, 从而可预防侧信道攻击。这里主要针对简单功耗分析攻击 (Simple Power Analysis, SPA)。由于芯片在运行不同的指令时消耗的功率不一样, 若算法迭代每步计算量不一致, 则攻击者可利用高分辨率功率测量仪器从外部测量芯片功率的变化, 进而提取部分或全部密钥以达到攻击的目的。

(3) *w*-坐标与标准的椭圆曲线有理点 (*x*, *y*)-坐标相比, 不仅减少了群律计算和同源计算中的中间计算量(少算一个坐标), 还可以节省一半的带宽。如在 ECC 中取素数 NIST p256 的情况下, 可将传递的有理点参数从 512 bit 节省到 256 bit; 在 SIKE 中取素数为 p434 的时候, 可将传递的有理点参数从 1736 bit 减少为 868 bit.

当然, *w*-坐标也存在不足之处: 由于它诱导的椭圆曲线群律运算并不完备, 更多的时候我们将其称为“伪”群律运算。但我们可以通过一些特殊的处理方式弥补这一短处, 从而有效的支持相关计算。

1.3 本文工作

目前已有的关于椭圆曲线上 *w*-坐标的构造根据所选择的曲线模型有所不同。由于 Edwards, Huff, Jacobi 等曲线模型在某些条件下可与 Montgomery 曲线模型建立双有理等价映射, 因此若能在 Montgomery 曲线模型上开发出更多的 *w*-坐标, 则其他曲线模型可得到更多 *w*-坐标的选择, 从而设计更优的算法。

本文基于前述文献工作基础, 提出利用 Montgomery 曲线上的 2-同源构造出 3 类新的 *w*-坐标。与 *x*-坐标相同的是, 它们均可应用于 Montgomery ladder 算法。更进一步的, 这类 *w*-坐标技术可用于奇数次同源计算的优化, 包括同源映射的像以及目标同源曲线参数相关计算。

本文结构如下: 第 2 节主要介绍了本文需要用到的预备知识; 第 3 节主要介绍了其他曲线模型上已知的 *w*-坐标, 并描述了它们对于同源密码的优化; 第 4 节描述了本文的主要工作, 通过 2-同源复合 *x*-坐标得到新的 *w*-坐标; 第 5 节中我们研究了如何将 *w*-坐标用于同源的计算。

2 预备知识

2.1 Montgomery 曲线上的群律

设定义在域 F_q (特征不为 2, 3)上的 Montgomery 曲线 E[6]为

$$E: By^2 = x^3 + Ax^2 + x$$

其中参数 A 和 B 是域 F_q 上的值, 满 $B \neq 0$, $A^2 \neq 4$. 若令 $x = X/Z$, $y = Y/Z$,则对应投影模型

$$E: BY^2Z = X^3 + AX^2Z + XZ^2$$

无穷远点为 $\Theta = (0:1:0)$.

结论 1.取 E 上两点 $P_1 = (x_1, y_1)$, $P_2 = (x_2, y_2)$, 设 $P_1 + P_2 = (x_3, y_3)$, $P_1 - P_2 = (x_4, y_4)$. 则由群律公式[6]可得

$$\begin{aligned} x_3x_4 &= (x_1x_2 - 1)^2 / (x_1 - x_2)^2, \\ x_3 + x_4 &= \frac{2\left[(1 + x_1x_2)(x_1 + x_2) + 2Ax_1x_2\right]}{(x_1 - x_2)^2}. \end{aligned} \tag{1}$$

当 $x_1x_2 = 0$ 时, 上述等式依旧成立.若 $P_1 = P_2$,有

$$x_3 = (x_1^2 - 1)^2 / 4x_1(x_1^2 + Ax_1 + 1). \tag{2}$$

2.2 2-同源的计算

根据 Vélu 公式[15], 已知同源映射的核, 即得到同源公式与像曲线的系数。不妨设 T 是 E 的 2 阶点, 即 $T = (0,0)$, $T = (a,0)$ 或 $T = (1/a, 0)$, 其中

$$a = \frac{-A + \sqrt{A^2 - 4}}{2}.$$

定理 1. 根据 Vélu 公式[15]可得, Montgomery 曲线 E 上以 2-阶点所生成的子群为核的 2-同源公式.

第一, 以 $\langle (0,0) \rangle$ 为核:

$$\phi_1(x,y) \to \left(\frac{(x-1)^2}{2\sqrt{2+A}x}, \frac{y}{2\sqrt{2+A}}\left(1 - \frac{1}{x^2}\right) \right)$$

像曲线 $E_1: \frac{B}{2\sqrt{2+A}} y^2 = x^3 + \frac{A+6}{2\sqrt{2+A}} x^2 + x$;

第二, 以 $\langle (a,0) \rangle$ 为核:

$$\phi_2(x,y) \to \left(\frac{x(ax-1)}{(2a^2-1)(x-a)}, y + \frac{y(a^2-1)}{(x-a)^2} \right)$$ 像曲线 $E_2: \frac{B}{(2a - 1/a)^3} y^2 = x^3 - 2x^2 + x$;

第三, 以 $\langle (1/a, 0) \rangle$ 为核:

$$\phi_3(x,y) \to \left(\frac{a^2x(x-a)}{(2-a^2)(ax-1)}, y + \frac{y(1-a^2)}{(ax-1)^2} \right)$$

像曲线 $E_3: \frac{B}{(2/a - a)^3} y^2 = x^3 - 2x^2 + x$.

证明. 若以 $\langle (0,0) \rangle$ 为核, 则由 Vélu 公式有

$$F_1: By^2 = x^3 + (A+6)x^2 + 4(2+A)x,$$

$$\psi_1: E \to F_1,$$

$$(x,y) \mapsto \left(\frac{(x-1)^2}{x}, y\left(1 - \frac{1}{x^2}\right) \right).$$

由于 F_1 是 Weierstrass 型曲线, 于是据 F_1 可构造

同构映射 ψ_2, 将 F_1 转换成 Montgomery 曲线.

$$\psi_2 : F_1 \to E_1,$$

$$(x,y) \mapsto \left(\frac{x}{2\sqrt{2+A}}, \frac{y}{2\sqrt{2+A}} \right).$$

于是 $\phi_1 = \psi_2 \circ \psi_1$.

若以 $\langle (a,0) \rangle$ 为核, 则由 Vélu 公式有

$$F_2 : By^2 = x^3 - \left(4a + \frac{1}{a} \right) x^2 + \left(4 + 4a^2 \right) x - 4a,$$

$$\varphi_1 : E \to F_2,$$

$$(x,y) \to \left(x + \frac{ax-1}{x-a}, y + \frac{y\left(a^2-1\right)}{(x-a)^2} \right).$$

同理, 可构造同构映射将 F_2 转换成 Montgomery 曲线模型.

$$F_3 : By^2 = x^3 + \left(\frac{2}{a} - 4a \right) x^2 + \left(2a - \frac{1}{a} \right)^2 x,$$

$$\varphi_2 : F_2 \to F_3,$$

$$(x,y) \mapsto \left(x - \frac{1}{a}, y \right),$$

$$\varphi_3 : F_3 \to E_2$$

$$(x,y) \mapsto \left(\frac{x}{2a - 1/a}, y \right).$$

因此 $\phi_2 = \varphi_3 \circ \varphi_2 \circ \varphi_1$.

同理可得以 $\langle (1/a, 0) \rangle$ 为核的 2-同源.

3 椭圆曲线上的 *w*-坐标

如同引言中提到的, Montgomery 曲线模型 (E,Θ) 上的 x-坐标诱导了从 $E/\{\pm 1\}$ 到射影直线 $\boldsymbol{P}$(即 Kummer 线,设为 K_E^{Θ})的同构映射, 因此椭圆曲线算术可以只用 x-坐标进行, 从而达到简化计算的目的。为了在其他曲线模型上达到和 Montgomery 曲线上 x-坐标类似的群律计算公式, 人们提出了 w-坐标可诱导其他曲线模型到射影直线 $\boldsymbol{P}$ 的双射。目前已知其他曲线上的 w-坐标如下所述。

在 twisted Edwards 曲线模型[11]

$$E_{TE} : ax^2 + y^2 = 1 + dx^2y^2$$

其中, Farashahi 和 Hossei 为了优化群律计算同时应用 Montgomery ladder 算法, 提出了 Edwards 曲线模型上的 w-坐标[11], 具体如下

令 $w(x,y) = d(xy)^2$. 设 $P,Q \in E_{TE}$, 令 $w_1 = w(P)$, $w_2 = w(Q)$, $w_3 = w(P+Q)$, $w_0 = w(P-Q), w_4 = w([2]P)$. 则有

$$w_4 = \frac{4w_1\left((w_1+1)^2 - ew_1 \right)}{\left(w_1^2 - 1 \right)^2},$$

$$w_3 w_0 = \frac{(w_1 - w_2)^2}{(w_1 w_2 - 1)^2}.$$

其中 $e = 4a/d$. Farashahi 等人利用这种 w-坐标将倍-加运算的计算量减少为 6M+4S+1D, 其中 M,S,D 分别表示乘法, 平方和常数乘法。同时他们还提出 twisted Edwards 曲线模型上另外几种 w-坐标

$w(x,y) = a(x/y)^2$, $w(x,y) = \sqrt{ad}\left(\frac{2x}{ax^2+y^2} \right)^2$ 等。

随后 Kim 等人[12]将上述结果应用到了 Edwards 曲线上奇数次同源的计算中, 并验证了奇数次同源的计算中 Edwards 曲线比 Montgomery 曲线在实际速度中更加突出, 且在曲线参数的传递上比 Montgomery 更有优越性。在应用 w-坐标之后, CSIDH (基于 SIDH 的一种变种密码方案)的实现比之前提高了 20%.

由于 Montgomery 和 Edwards 曲线上的高效群律和同源计算公式, 所以目前大部分关于 SIDH 的实现中主要选择这两类曲线模型。

Huang 等人[13]在 Huff 曲线模型

$$H_{a,d} : ax\left(y^2 - 1\right) = by\left(x^2 - 1\right)$$

上提出了一类新的 w-坐标, 并利用 w-坐标优化了 Huff 曲线上的群律计算, 将倍-加运算量减少为 6M+4S+1D, 加快了约 40%. 同时在 2-同源和奇数次同源的计算中, 利用 w-坐标之后运算量减少了约 50%, 将 Huff 曲线上的运算量减少到了与 Montgomery 曲线相同。 Drylo 等人[14]在 Huff 曲线上也得到了类似结果。

例如, 令 $w(x,y) = \frac{1}{xy}$. 设 $P,Q \in H_{a,d}$, 且 $w_i, i = 0,\cdots,4$ 如 Edwards 曲线所设, 则有

$$w([2]P) = \frac{\left(w_1^2 - 1 \right)^2}{4w_1\left(w_1 + c \right)\left(w_1 + \frac{1}{c} \right)},\ w_3 w_0 = \left(\frac{w_1 w_2 - 1}{w_1 - w_2} \right)^2.$$

综上所述, 使用 w-坐标可优化不同曲线模型上的群律计算, 对于不同椭圆曲线模型上的 w-坐标与普通坐标的倍-加运算量对比结果如下表。

表 1 倍-加运算运算量对比

Table 1 The Comparison of Computational Costs of Double-and-Add Operation

	普通坐标	w-坐标
Montgomery[2]	6M+4S	6M+4S
Edwards[11]	6M+3S+3D	6M+4S+1D
Huff[13]	10M+2S	5M+4S+1D
Hessian[10]	12M+6S+1D	/
Jacobi quartic[16]	5M+4S+5D	/
Jacobi intersection[17]	13M+6S+4D	/

由于在Montgomery曲线模型上的x-坐标可以作为 w-坐标, 所以运算量没有明显的改变。但从上表可以看出, 在其他曲线模型上使用 w-坐标可以得到与 Montgomery 曲线模型类似的群律算法。最后三类曲线上的 w-坐标还有待研究。

4 Montgomery 曲线上的 w-坐标

在同一曲线模型中, 利用 Hisil 和 Renes 的方法[16], 我们可以通过加上 2 阶点平移的方式得到更多的 w-坐标。例如在 Montgomery 曲线模型上可以将 x-坐标看成一种 w-坐标, 再通过2阶点的加法得到一类新的 w-坐标[18]。

设 Montgomery 曲线模型(E,Θ)上的任意一点$P=(x,y)$,由于 w-坐标将(E,Θ)映射到x轴, 即

$$w: E \to \mathrm{P}^1$$

$$(X:Y:Z)\mapsto \begin{cases}(X:Z) & if \quad Z\neq 0\\ (1:0) & if \quad Z=0\end{cases},$$

记 Kummer 线为 K_E^{Θ}.

如同第二节, 不妨设有 2-阶点$T\in(E,\Theta)$, 即有$[2]T=\Theta$. 通过 2-阶点的平移可得

$$\tau_T:(E,\Theta)\to(E,T)$$

$$P\mapsto P+T$$

显然 τ_T 是同构映射。w-坐标将 Montgomery 曲线(E,T)映射到$(E,T)/\{\pm 1\}$,记为 K_E^T. 则有如下关系

$$\begin{array}{ccc}(E,\Theta) & \xleftrightarrow{\tau_T} & (E,T)\\ \downarrow w & & \downarrow w\\ K_E^{\Theta} & \xleftrightarrow{\bar{\tau}_T} & K_E^T\end{array}$$

其中 τ_T 是 K_E^{Θ} 与 K_E^T 之间的同构映射。例如, 若令 $T=(0,0)$ 有 $\bar{\tau}_{(0,0)}:(X:Z)\mapsto(Z:X)$.从而通过加$T$平移得到的 w-坐标为 $w(P)=1/x$.

若 $T=(a,0)$, 可得 $w(P)=\dfrac{ax-1}{x-a}$.同理, 若 $T=\left(\dfrac{1}{a},0\right)$, 则 $w(P)=\dfrac{x-a}{ax-1}$.

本文提出在 Montgomey 曲线 $w-$坐标上复合 2-同源 ϕ, 可以得到新的 w-坐标, 即有

$$\begin{array}{ccc}(E,\Theta) & \xrightarrow{\phi} & (E',\Theta)\\ \downarrow w & & \downarrow w\\ K_E^{\Theta} & \xrightarrow{\phi'} & K_{E'}^{\Theta}\end{array}$$

其中 E' 的 Kummer 线记为 $K_{E'}^{\Theta}$, ϕ' 表示 K_E^{Θ} 到 $K_{E'}^{\Theta}$ 之间的同态映射。

对于 E 上 2 阶点 Q 生成的子群 $\langle Q\rangle=\{Q,\Theta\}$ 的陪集, 因为 $w(P+Q)$ 对于差分加法满足平行四边形法则[6], 所以 $w(P+\langle Q\rangle)$ 仍满足平行四边形法则。 由 2-同源 ϕ 是同态的, 于是复合可得 E 上新的 $w-$坐标 $w'=w\circ\phi$.

由定理 1 中 ϕ_1 可复合得到 $w'(P)=\dfrac{(x-1)^2}{2\sqrt{A+2x}}$.以下推论可证明新得到的 w-坐标满足平行四边形法则[6], 因此可以用于 Montgomery ladder 算法和同源计算, 如下节所示。

推论 2. 设 $E\setminus(0,0)$ 上任意两点 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$. 令 $w_1=w'(P_1)$, $w_0=w'([2]P_1)$, $w_3=w'(P_1+P_2)$, $w_4=w'(P_1+P_2)$. 则有

$$w_0=\frac{\left(w_1^2-1\right)^2}{4w_1\left(w_1^2+\dfrac{6+A}{2\sqrt{2+A}}w_1+1\right)}. \tag{3}$$

$$w_3w_4=\frac{\left(w_1w_2-1\right)^2}{\left(w_1-w_2\right)^2} \tag{4}$$

证明. 设 $[2]P_1=(x_{2P},y_{2P})$, $P_1+P_2=(x_3,y_3)$ 以及 $P_1-P_2=(x_3,y_3)$. 则由公式(1)得

$$w_0=\left(x_{2P}-1\right)^2\Big/\left(2\sqrt{2+A}x_{2P}\right)$$

$$=\frac{\left[\left(x_1^2-1\right)^2\Big/4x_1\left(x_1^2+Ax_1+1\right)-1\right]^2}{2\sqrt{2+A}\left(x_1^2-1\right)^2\Big/4x_1\left(x_1^2+Ax_1+1\right)}$$

$$=\frac{\left[(x_1-1)^4-\left(2\sqrt{2+A}x_1\right)^2\right]^2}{4(x_1-1)^2\left(2\sqrt{2+A}x_1\right)\left[(x_1-1)^4+(6+A)x_1(x_1-1)^2+1\right]^2}$$

$$=\frac{\left[\dfrac{(x_1-1)^4}{2\sqrt{2+A}x_1}-1\right]^2}{4\dfrac{(x_1-1)^2}{2\sqrt{2+A}x_1}\left[\dfrac{(x_1-1)^4}{\left(2\sqrt{2+A}x_1\right)^2}+\dfrac{6+A}{2\sqrt{2+A}}\cdot\dfrac{(x_1-1)^2}{2\sqrt{2+A}x_1}+1\right]}$$

$$=\frac{\left(w_1^2-1\right)^2}{4w_1\left(w_1^2+\dfrac{6+A}{2\sqrt{2+A}}w_1+1\right)}$$

类似, 由公式(2)可得

$$w_3w_4=\frac{\left[(x_1-1)^2(x_2-1)^2-4(2+A)x_1x_2\right]^2}{\left[2\sqrt{2+A}x_2(x_1-1)^2-2\sqrt{2+A}x_1(x_2-1)^2\right]}$$

$$=\frac{\left[\dfrac{(x_1-1)^2(x_2-1)^2}{4(2+A)x_1x_2}-1\right]^2}{\left[\dfrac{(x_1-1)^2}{2\sqrt{2+A}x_1}-\dfrac{(x_2-1)^2}{2\sqrt{2+A}x_2}\right]^2}=\frac{(w_1w_2-1)^2}{(w_1-w_2)^2}.$$

Montgomery 曲线模型上共有 3 种 2-同源, 不同的同源复合可得到不同的 *w*-坐标。由于 2-同源公式有三个, 则由定理 2 的 ϕ_2 可得

$$w'(P)=\frac{x(ax-1)}{(2a^2-1)(x-a)}.$$

则同样类似推论 2, 可证明上述 *w*-坐标的运算满足平行四边形法则:

推论 3. 设 $E\setminus(a,0)$, 上任意两点 $P_1=(x_1,y_1)$, $P_2=(x_2,y_2)$. 令 $w_1=w'(P_1)$, $w_0=w'([2]P_1)$, $w_3=w'(P_1+P_2)$, $w_4=w'(P_1+P_2)$. 则有

$$w_0=\frac{\left(w_1^2-\dfrac{1}{\left(2a^2-1\right)^2}\right)^2}{4w_1\left(w_1^2-2w_1+\dfrac{1}{2a^2-1}\right)} \tag{5}$$

$$w_3w_4=\frac{\left(w_1w_2-\dfrac{1}{\left(2a^2-1\right)^2}\right)^2}{\left(w_1-w_2\right)^2} \tag{6}$$

证明. 同样设 $[2]P_1=(x_{2P},y_{2P})$, $P_1+P_2=(x_3,y_3)$ 以及 $P_1-P_2=(x_3,y_3)$. 则由(2.1)得

$$w_0=\frac{x_{2P}(ax_{2P}-1)}{\left(2a^2-1\right)\left(x_{2P}-a\right)},$$

$$=\frac{(x_1-1)^2(x_1+1)^2\left(ax_1^2+a-2x_1\right)^2}{4\left(2a^2-1\right)x_1(ax_1-1)\left(x_1^2-2ax_1+1\right)^2},$$

$$=\frac{\left(w_1^2-\dfrac{1}{\left(2a^2-1\right)^2}\right)^2}{4w_1\left(w_1^2-2w_1+\dfrac{1}{2a^2-1}\right)}.$$

类似, 由公式(2)可得

$$w_3w_4=\frac{x_3x_4\left[ax_3x_4-a\left(x_3+x_4\right)+1\right]}{\left(2a^2-1\right)^2\left[x_3x_4-a\left(x_3+x_4\right)+a^2\right]},$$

$$=\frac{\left(x_1x_2-1\right)^2\left[(ax_2-1)x_1-x_2+a\right]^2}{\left(2a^2-1\right)\left(x_1-x_2\right)^2\left[(a-x_2)x_1+ax_2-1\right]^2},$$

$$=\frac{\left(w_1w_2-\dfrac{1}{\left(2a^2-1\right)^2}\right)^2}{\left(w_1-w_2\right)^2}.$$

同时, 可将推论 3 中的等式进一步简化成 $w'(P)=\dfrac{x(ax-1)}{(x-a)}$, 则有以下结论

$$w_0=\frac{\left(w_1^2-1\right)^2}{4w_1\left(w_1^2-2\left(2a^2-1\right)w_1+1\right)} \tag{7}$$

$$w_3w_4=\frac{(w_1w_2-1)^2}{(w_1-w_2)^2} \tag{8}$$

同理, 定理 1 的 ϕ_3 得 $w'(P)=\dfrac{a^2x(x-a)}{\left(2-a^2\right)(ax-1)}$, 类似推论 3 的证明有

$$w_0=\frac{\left[w_1^2-\dfrac{a^4}{\left(a^2-2\right)^2}\right]^2}{4w_1\left(w_1^2-2w_1+\dfrac{a^4}{\left(a^2-2\right)^2}\right)} \tag{9}$$

$$w_3w_4=\frac{\left(w_1w_2-\dfrac{a^4}{\left(a^2-2\right)^2}\right)^2}{\left(w_1-w_2\right)^2} \tag{10}$$

可将上述 $w-$ 坐标化简, 令 $w'(P)=\dfrac{x(x-a)}{(ax-1)}$, 则有

$$w_3w_4=\frac{\left(w_1w_2-1\right)^2}{\left(w_1-w_2\right)^2} \tag{11}$$

$$w_0=\frac{\left(w_1^2-1\right)^2}{4w_1\left(w_1^2-\dfrac{2\left(2-a^2\right)}{a^2}w_1+1\right)} \tag{12}$$

在实际计算中, 可将上述公式转为射影坐标和射影系数形式。以 $w'(P)=\dfrac{(x-1)^2}{2\sqrt{A+2x}}$ 为例, 令 $d=\dfrac{6+A}{2\sqrt{2+A}}$, 设 $D=\dfrac{d+2}{4}$, $w_i=W_i/Z_i$, 其中 $i=0,1,2,3$. 则有算法 1 计算倍-加运算如下:

算法 1.xDBLADD.

输入: W_1, Z_1, W_2, Z_2, w_4, D

输出: W_0, Z_0, W_3, Z_3

$t_0=W_1+Z_1$; $t_1=W_1-Z_1$; $W_0=t_0^2$;

$t_2=W_2-Z_2$; $W_3=W_2+Z_2$; $t_0=t_0\cdot t_2$;

$Z_0=t_1^2$; $t_1=t_1\cdot W_3$; $t_2=W_0-Z_0$; $W_0=W_0\cdot Z_0$;

$W_3=D\cdot t_2$; $Z_3=t_0-t_1$; $Z_0=W_3+Z_0$;

$W_3=t_0+t_1$; $Z_0=Z_0\cdot t_2$; $Z_3=Z_3^2$; $W_3=W_3^2$;

$Z_3=w_4\cdot Z_3$;

RETURN W_0, Z_0, W_3, Z_3;

算法 1 的计算量为 6M+4S+2a. 其中 M, S, a 分别代表乘法, 平方, 加法。与文献[19]中利用 Montgomery 曲线的 x-坐标计算量保持一致。

同样以 $w'(P)=\dfrac{(x-1)^2}{2\sqrt{A+2x}}$ 为例, 设 k 为私钥, $w'([2P_1])=W_0/Z_0$, $w'([k]P_1)=W_k/Z_k$. 将 w' 应用到 Montgomery ladder 算法作标量乘运算如下:

算法 2. Montgomery ladder.

输入: $k=\sum_{i=0}^{\ell-1}k_i2^i$ 且 $k_{\ell-1}=1$, D, W_1, Z_1, W_0, Z_0, $w'(P_1)$

输出: W_k, Z_k

1 FOR $i=\ell-2$ DOWN TO 0 DO

2 IF $k_i=0$ THEN

3 (W_1,Z_1,W_0,Z_0)=xDBLADD($W_1,Z_1,W_0,Z_0,w'(P_1),D$)

4 ELSE

5 (W_0,Z_0,W_1,Z_1)=xDBLADD($W_1,Z_1,W_0,Z_0,w'(P_1),D$)

6 RETUEN W_1,Z_1

采用 w-坐标的算法 2 计算量与采用 x-坐标的 Montgomery ladder 算法计算量一致。

由于在其他曲线模型上采用 w-坐标, 可得到 Montgomery 曲线模型上类似的群律计算公式, 于是同样可以利用 Montgomery ladder 算法抵抗侧信道攻击。

例如, 利用 Montgomery 曲线与 twisted Edwards 曲线之间存在同构映射[2]

$$\phi:(x,y)\mapsto\left(\frac{x}{y},\frac{x-1}{x+1}\right),$$

$$\phi^{-1}:(x,y)\mapsto\left(\frac{1+y}{1-y},\frac{1+y}{x(1-y)}\right).$$

所以通过 twisted Edwards 曲线模型 (E_{TE},Θ) 上的 y-坐标同样可以作为 w-坐标。并且可建立 K_E^{Θ} 与 K_{TE}^{Θ} 之间的映射 $\bar{\phi}(x)=\dfrac{1+y}{1-y}$.

由于 w-坐标群律运算只是一种“伪”群律计算, 所以并不完备, 但这并不影响我们将其应用到同源计算中。

5 奇数次同源的计算

同源密码中奇数次同源的计算十分关键。例如在 SIKE 中需要多次计算 3-同源。在 Castryck 等人[20]提出的基于 SIDH 改进的同源密码方案 CSIDH 中, 则需要计算一些规模更大的奇数次同源。CSIDH 中选择的素数域特征形为 $p=4\cdot\ell_1\cdots\ell_n-1$, 其中 ℓ_i 是互不相同的小素数, 设私钥为 $(e_1,e_2,\cdots,e_n)$, $S=\{i|e_i\neq0,\mathrm{sign}(e_i)=s\}$, $k=\prod_{i\in S}\ell_i$, 其中当随机选择的点的纵坐标 y 在 F_p 上时 $s=1$ 否则 $s=-1$. 在生成公钥的迭代中需要多次计算 ℓ_i-同源, 其中 $i\in S$.

最终得到 $\ell^{e_1}\cdots\ell^{e_n}$ 次同源. 而在Costello提出的基于同源的密码方案 BSIDH 中[21], 则给出的一个素数域特征例子为 $p=2^{450}-2^{225}-1$, 此时 Bob 需要计算奇数次的 N-同源, 其中 N 有如下分解:

$$N=3^4\cdot5\cdot7\cdot11\cdot17\cdot19\cdot29\cdot31\cdot43\cdot73\cdot113\cdot127$$
$$\cdot151\cdot251\cdot257\cdot331\cdot449\cdot601\cdot631\cdot1801\cdot2689$$
$$\cdot4051\cdot5153\cdot23311\cdot65537\cdot100801\cdot115201.$$

Costello 和Hisil给出了一般情况下Montgomery曲线模型上的同源计算公式[22]如下:

定理 2[22]. 设 P 是曲线 E 上 $\ell=2d+1$ 阶点, 则有核 $\ker(\varphi)=\langle P\rangle$ 的 $\ell-$同源 $\varphi:E\to E'$,

$$E':B'y^2=x^3+A'x^2+x$$
$$A'=(6\tilde{\sigma}-6\sigma+A)\cdot\pi^2,\quad B'=B\cdot\pi^2$$

其中 $\sigma=\sum_{i=1}^{d}x_{[i]P}$, $\tilde{\sigma}=\sum_{i=1}^{d}1/x_{[i]P}$, $\pi=\prod_{i=1}^{d}x_{[i]P}$.

且有

$$\varphi:(x,y)\mapsto\left(f(x),y\cdot f'(x)\right)$$

其中 $f(x)=x\cdot\prod_{i=1}^{d}\left(\frac{x\cdot x_{[i]P}-1}{x-x_{[i]P}}\right)^2$, 导数为 $f'(x)$.

类似的, 利用第 4 节中得到的 *w*-坐标和 Vélu 公式可以得到关于 *w*-坐标的同源公式。实际上, 利用 *w*-坐标得到的奇数次同源计算公式, 与上述 Montgomery 曲线模型上的同源计算公式在形式上保持一致。

推论 4. 设 P 是曲线 E 上 $\ell=2d+1$ 阶点, 由定理 2, 可生成以 $\langle P\rangle$ 为核的 $\ell-$同源 φ, 设点 Q 满足 $Q=(x,y)\in E\setminus\langle P\rangle$, 且有 $w'(Q)=\frac{(x-1)^2}{2\sqrt{A+2x}}$, 则

$$\varphi\left(w'(Q)\right)=w'(Q)\prod_{T\in\langle P\rangle\setminus\{\Theta\}}w'(Q+T)\tag{13}$$

证明. 由于 $\langle P\rangle$ 为 ℓ 阶循环子群. 则当 $i\leqslant d$, 有

$$w'\left(Q+[\ell-i]P\right)=w'\left(Q-[i]P\right).$$

于是

$$w'(Q)\prod_{T\in\langle P\rangle\setminus\{\Theta\}}w'(Q+T)=w'(Q)\prod_{i=1}^{\ell}w'\left(Q+[i]P\right),$$
$$=w'(Q)\prod_{i=1}^{d}w'\left(Q+[i]P\right)w'\left(Q-[i]P\right),$$
$$=w'(Q)\prod_{i=1}^{d}\frac{\left(w'(Q)w'([i]P)-1\right)^2}{\left(w'(Q)-w'([i]P)\right)^2}=\varphi\left(w'(Q)\right),$$

需要注意的是, 由于第 4 节中的 *w*-坐标或利用平移 2 阶点得到, 或利用 2-同源得到, 因此在计算奇数次同源时并无影响, 但在计算偶数次同源时并不适用(但定理 2 中的公式没有限定同源次数的奇偶性)。

在同源计算中我们不仅需要计算同源映射的像, 还需要计算像曲线系数。由于在定理 2 中像曲线 E' 的系数 A' 的直接计算效率太低, 可以利用 Montgomery 曲线 E 的系数 A 与曲线上 2 阶点 $(a,0)$ 的关系 $A=-a-\frac{1}{a}$ 提高效率[19]。利用奇数次同源作用 2 阶点 $(a,0)$ 之后的像点 $(\hat{a},0)$ 仍然是像曲线 E' 上的 2-阶点, 同时像曲线系数 $A'=-\hat{a}-\frac{1}{\hat{a}}$, 其中

$$\hat{a}=a\prod_{i=1}^{d}\left(\frac{ax_{[i]P}-1}{a-x_{[i]P}}\right)^2.\tag{14}$$

同时 Montgomery 曲线 E 的 $j-$不变量同样可以由 2 阶点计算

$$j(E)=\frac{256\left(a^4-a^2+1\right)^3}{a^4(a-1)^2(a+1)^2}.\tag{15}$$

在实际的计算中, 可以以传递 2 阶点的坐标参数 *a*, 来代替椭圆曲线系数 *A*, 从而达到提高计算效率的目的。

此外, 我们还得到了如下两类同源计算优化方法可推广至 *w*-坐标情形(不限于 Montgomery 曲线模型):

(1) Costello 和 Hisil 提出的利用 3 差分点还原同源曲线参数的方法[22], 利用 *x*(*P*), *x*(*Q*), *x*(*P*-*Q*) 坐标可表示像曲线参数 A'。

$$A'=\frac{\left(1-x_Px_Q-x_Px_{Q-P}-x_Qx_{Q-P}\right)^2}{4x_Px_Qx_{Q-P}}-x_P-x_Q-x_{Q-P}$$

由于 *w*-坐标与 Montgomery 曲线上的 *x*-坐标一样满足差分加法, 因此关于 *w*-坐标也可得到类似的结果。

(2) Bernstein 等人在 $O(\sqrt{\ell})$ 量级计算量内计算同源映射和同源曲线参数的方法[23]。设 P 是奇数 ℓ 阶点, 令

$$S=\{1,3,\cdots,\ell-2\},\quad h_S(X)=\prod_{s\in S}\left(X-x([s]P)\right),$$

则有同源公式[23]

$$\varphi_x(X)=\frac{X^\ell\cdot h_S(1/X)^2}{h_S(X)^2}.$$

可由 Montgomery 曲线系数与 twisted Edwards

曲线系数 d 的关系[24], 求解像曲线系数

$$A' = 2(1+d)/(1-d)$$

其中

$$d = \left(\frac{A-2}{A+2}\right)^{\ell}\left(\prod_{s\in S}\frac{x([s]P)-1}{x([s]P)+1}\right)^{8}$$

$$= \left(\frac{A-2}{A+2}\right)^{\ell}\left(\frac{h_S(1)}{h_S(-1)}\right)^{8}.$$

因此可利用 SIMD 指令集将坐标计算和系数计算并行化处理, 从而得到同源密码实现的进一步加速。注意到公式(13)和(14)计算公式与上述公式在形式上一致, 将上述公式中的 w-坐标换成 w-坐标同样可得到类似的结果。

6 结论

本文研究了可用于高效安全计算椭圆曲线群律运算和同源映射的 w-坐标技术, 通过总结目前在各类椭圆曲线模型(其中重点考查 Montgomery 模型)上的 w-坐标及其相关计算, 分析其特点与带来的计算上的优势。特别的, 我们采用 Montgomery 曲线模型上的 2-同源, 与已知的 w-坐标进行复合, 得到三种新的 w-坐标, 对它们诱导的群律进行了推导, 最后将其应用到了奇数次同源的计算优化上。而对于其他曲线模型上的 w-坐标, 同样可以利用类似技巧进行重新构造, 未来期待能利用新的 w-坐标进一步支持或优化同源密码中的计算, 从而推动超奇异同源密码走向实际应用。

参考文献

[1] Shor P W. Algorithms for Quantum Computation: Discrete Logarithms and Factoring[C]. *The 35th Annual Symposium on Foundations of Computer Science*, 1994: 124-134.

[2] F Jao D, Feo L. Towards Quantum-Resistant Cryptosystems from Supersingular Elliptic Curve Isogenies [J]. *Journal of Mathematical Cryptology*, 2014, 8:209-247.

[3] NIST. Post quantum crypto project. http://csrc.nist.gov/groups/NIST/post-quantum-crypto, 2020.

[4] Liu W Q, Ni J, Liu Z, et al. Optimized Modular Multiplication for Supersingular Isogeny Diffie-Hellman[J]. *IEEE Transactions on Computers*, 2019, 68(8): 1249-1255.

[5] Tian J, Lin J, Wang Z F. Fast Modular Multipliers for Supersingular Isogeny-Based Post-Quantum Cryptography[J]. *IEEE Transactions on Very Large Scale Integration* (*VLSI*) *Systems*, 2021, 29(2): 359-371.

[6] Montgomery P L. Speeding the Pollard and Elliptic Curve Methods of Factorization[J]. *Mathematics of Computation*, 1987, 48(177): 243.

[7] Koziel B, Azarderakhsh R, Kermani M M. A High-Performance and Scalable Hardware Architecture for Isogeny-Based Cryptography[J]. *IEEE Transactions on Computers*, 2018, 67(11): 1594-1609.

[8] Koziel B, Ackie A B, Khatib R E, et al. SIKE'd Up: Fast Hardware Architectures for Supersingular Isogeny Key Encapsulation[J]. *IEEE Transactions on Circuits and Systems I*: *Regular Papers*, 2020, 67(12): 4842-4854.

[9] Karati S, Sarkar P. Kummer for Genus one over Prime-Order Fields[J]. *Journal of Cryptology*, 2020, 33(1): 92-129.

[10] Farashahi R R, Joye M. Efficient Arithmetic on Hessian Curves[M]. Public Key Cryptography – PKC 2010. Berlin, Heidelberg: Springer Berlin Heidelberg, 2010: 243-260.

[11] Farashahi R R, Hosseini S G. Differential Addition on Twisted Edwards Curves [C]. *Australasian Conference on Information Security and Privacy*, 2017: 366-378.

[12] Kim S, Yoon K, Park Y H, et al. Optimized Method for Computing Odd-Degree Isogenies on Edwards Curves[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2019: 273-292.

[13] Huang Y, Zhang F G, Hu Z, et al. Optimized Arithmetic Operations for Isogeny-Based Cryptography on Huff Curves[C]. *Australasian Conference on Information Security and Privacy*, 2020:23-40.

[14] Drylo R, KijkoT, Wronski M. Efficient Montgomery-like formulas for general Huff's and Huff's elliptic curves and their applications to the isogeny-based cryptograph[EB/OL]. 2020:Cryptology ePrint Archive:2020/526.

[15] Vélu J. Isogénies Entre Courbes Elliptiques[J]. *CR Acad. Séci. Paris Sr. AB*, 1971, 273: A238–A241.

[16] Gu H H, Xie W L, Gu D W. Differential Addition on Jacobi Quartic Curves[C]. *Symposium on ICT and Energy Efficiency and Workshop on Information Theory and Security*, 2012: 194-197.

[17] H Hişil. Elliptic Curves, Group Law, and Efficient Computation[D]. Queensland University of Technology, 2010.

[18] Hisil H, Renes J. On Kummer Lines with Full Rational 2-Torsion and Their Usage In Cryptography[J]. *ACM Transactions on Mathematical Software*, 2019, 45(4): 1-17.

[19] Costello C, Longa P, Naehrig M. Efficient Algorithms for Supersingular Isogeny Diffie-Hellman[C]. *Advances in Cryptology - CRYPTO 2016*, 2016:572-601.

[20] Castryck W, Lange T, Martindale C, et al. CSIDH: An Efficient Post-Quantum Commutative Group Action[M]. Lecture Notes in Computer Science. Cham: Springer International Publishing, 2018: 395-427.

[21] Costello C. B-SIDH: Supersingular Isogeny Diffie-Hellman Using Twisted Torsion[C]. *Advances in Cryptology - ASIACRYPT 2020*, 2020: 440-463.

[22] Costello C, Hisil H. A Simple and Compact Algorithm for SIDH with Arbitrary Degree Isogenies[M]. Advances in Cryptology – ASIACRYPT 2017. Cham: Springer International Publishing, 2017: 303-329.

[23] Bernstein D J, de Feo L, Leroux A, et al. Faster Computation of Isogenies of Large Prime Degree[J]. *Open Book Series*, 2020, 4(1):

39-55.

[24] Moody D, Shumow D. Analogues of Vélu's Formulas for Isogenies on Alternate Models of Elliptic Curves[J]. *Mathematics of Computation*, 2016, 85(300): 1929-1951.

陶铮 于 2018 年在中南大学大学信息与计算科学专业获得学士学位. 现在中南大学学校数学专业攻读硕士学位。研究领域为同源密码的计算. 研究兴趣包括: 同源密码的软件实现。Email: 192111043@csu.edu.cn

胡志 于2012 年在北京大学应用数学专业获得博士学位. 现任中南大学数学与统计学院副教授. 研究领域为密码学与信息安全. 研究兴趣包括：椭圆曲线密码、基于同源的后量子密码。Email：huzhi_ math@csu.edu.cn