第44卷第10期 中国科学技术大学学报 Vol. 44, No. 10
2014年10月 JOURNAL OF UNIVERSITY OF SCIENCE AND TECHNOLOGY OF CHINA Oct. 2014

文章编号:0253-2778(2014)10-0835-04

构造从字符串到 Huff 曲线的散列函数

于 伟[1,2],王鲲鹏[1],李 宝[1]

(1. 中国科学院信息工程研究所,北京 100093;2. 中国科学技术大学电子工程与信息科学系,安徽合肥 230027)

摘要:首次构造了从有限域 F_q 到 Huff 曲线的确定函数,其时间复杂性为 $O(\log^3 q)$. 在此基础上构造了从字符串到 Huff 曲线的散列函数. 该散列函数的构造为基于身份协议的构造奠定了基础. 其在中国椭圆曲线密码算法标准 SM2 推荐的素域上的运行时间为 557.8 μs.

关键词:散列函数;Huff 曲线;能量攻击;SM2

中图分类号:TP309 **文献标识码**:A doi:10.3969/j.issn.0253-2778.2014.10.006

引用格式: Yu Wei, Wang Kunpeng, Li Bao. Constructing hash function from plaintext to Huff curves[J]. Journal of University of Science and Technology of China, 2014,44(10):835-838.
于伟,王鲲鹏,李宝. 构造从字符串到 Huff 曲线的散列函数[J]. 中国科学技术大学学报,2014,44(10):835-838.

Constructing hash function from plaintext to Huff curves

YU Wei[1,2], WANG Kunpeng[1], LI Bao[1]

(1. *Institute of Information Engineering, Chinese Academy of Sciences, Beijing* 100093, *China*;
2. *Department of Electronic Engineering and Information Science, University of Science and Technology of China, Hefei* 230027, *China*)

Abstract: A deterministic function with its time complexity being $O(\log^3 q)$ was constructed for the first time from a finite field F_q to Huff curves. Based on this function, construct a hash function from plaintext into Huff curves. The Hash function laid the foundation for identity-based protocols on elliptic curves and its experimental time cost on the elliptic curve of the Chinese elliptic curve standard SM2 is 557.8 μs.

Key words: Hash function; Huff curve; power analysis; SM2

0 引言

1986 年,Koblitz[1] 和 Miller[2] 同时独立地提出了椭圆曲线密码学体制. 由于一般椭圆曲线上不存在亚指数的攻击算法,所以椭圆曲线密码体制的应用越来越广泛. 随着我国椭圆曲线密码标准 SM2 的发布,椭圆曲线密码体制在我国得到了进一步的应用. Joye 等[3] 在 2010 年给出了特征不为 2 的有限域上的 Huff 曲线,后来又给出了二进制域上的 Huff 曲线[4]. Huff 曲线具有有效的群律和加法倍点统一公式,可以抵抗能量攻击[5]. Wu 等[6] 推广了 Huff 形式的椭圆曲线.

Boneh-Frankin 构造的基于身份的加密算法[7] 中,公钥需要映射到椭圆曲线上的点. 他们构造了一

收稿日期:2013-09-10;**修回日期**:2014-05-01

基金项目:国家重点基础研究发展(973)计划(2013CB338001),中国高技术研究发展(863)计划(2013AA014002),国家自然科学基金(61272040,61070171),中国科学院战略性先导专项(XDA06010702)资助.

作者简介:于伟,男,1987 年生,博士. 研究方向:椭圆曲线密码学. E-mail:yuwei_1_yw@163.com

通讯作者:王鲲鹏,研究员/博士生导师. E-mail:kunpengwang@263.net

个从基域 F_q 到超奇异椭圆曲线上点的一一映射 f，可以证明当 h 是一个传统哈希函数时，$f(h(m))$ 也相当于一个传统哈希函数.其他的一些系统，如基于身份的加密算法[8]，基于身份的签名算法[9-11]、基于身份的签密算法[12-13]、Lindell 的普适组合承诺算法[14]等，都需要哈希进椭圆曲线.

文献[7]给出了一个概率算法计算到椭圆曲线的散列函数，该算法的执行时间不是常数，并且可能导致计时攻击.文献[15-18]讨论了以固定多项式时间构造从有限域 F_q 到 Weierstrass 形式椭圆曲线的散列函数；文献[19]讨论了构造到 Hessian 曲线的散列函数；文献[20]讨论了 Montgomery 曲线上散列函数的构造.

考虑到 Huff 曲线具有统一有效的群律，可以抵抗能量攻击.本文构造了到 Huff 曲线的确定性函数，并且在此基础上，构造了到 Huff 曲线的散列函数.实验表明该函数在 SM2 推荐的素域上只需要 557.8 μs.这也是第一次构造到 Huff 曲线的散列函数，并且该函数的效率很高.

1 素域上的 Huff 曲线

设 F_q 是特征大于 3 的有限域.

定义 1.1 定义 F_q 上的 Huff 形式椭圆曲线，简称 Huff 曲线，其方程 E_{ab} 为：

$$ax(by^2-1)=by(ax^2-1) \tag{1}$$

式中，$a,b\in F_q$，$a^2\neq b^2$，$a,b\neq 0$.

标准射影形式的 Huff 形式椭圆曲线方程为 $aX(Y^2-Z^2)=bY(X^2-Z^2)$.Huff 曲线的 3 个无穷远点为(1:0:0)，(0:1:0)，(a:b:0).我们给出实数域上 Huff 形式椭圆曲线的图形，如图 1 所示.

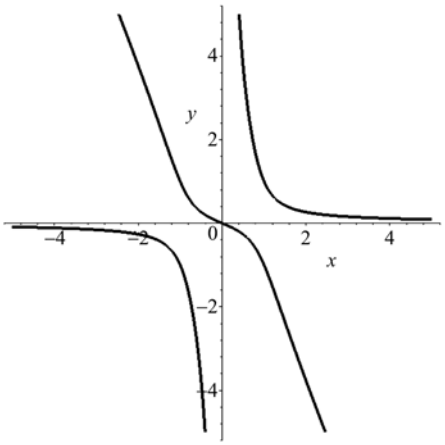

图 1 Huff 曲线 $3x(y^2-1)=-7y(x^2-1)$

Fig. 1 Huff curve $3x(y^2-1)=-7y(x^2-1)$

F_q 上的 Huff 曲线，$L\supseteq F_q$，其 L-有理点群一定包含一个子群同构于 $Z/4Z\times Z/2Z$，也就是说一定包含 2 阶和 4 阶点.并且任一定义在 F_q 上的包含子群 $Z/4Z\times Z/2Z$ 的椭圆曲线都双有理等价于一条定义在 F_q 上的 Huff 曲线.取单位元为(0:0:1)时，3 个无穷远点都为 2 阶点，4 个 4 阶点为{(1:1:1)，(1:−1:1)，(−1:1:1)，(−1:−1:1)}.这 8 个元素构成的子群同构于 $Z/4Z\times Z/2Z$[3].

2 构造从有限域到 Huff 曲线的确定性函数

当 $q=p^n\equiv 2 \bmod 3$ 时，映射 $x\mapsto x^3$ 是一个双射，并且有逆映射 $x\mapsto x^{1/3}=x^{(2q-1)/3}$.由此可以构造从 F_q 到 Huff 曲线的确定性映射.

该确定性映射 $f_{ab}:s\mapsto(x,y)$ 的构造如下：

$$\left.\begin{aligned}x&=\frac{b(u+a^2)}{su+v}\\ y&=\frac{a(u+b^2)}{su+v}\end{aligned}\right\} \tag{2}$$

式中，

$$u=-\frac{a^2+b^2-s^2}{3}+\sqrt[3]{v^2+\left(\frac{a^2+b^2-s^2}{3}\right)^3},$$

$$v=\frac{a^2b^2-3\left(\frac{a^2+b^2-s^2}{3}\right)^2}{2s}.$$

容易验证如式(2)构造的 x,y 满足 Huff 曲线方程 $ax(by^2-1)=by(ax^2-1)$.

下面给出该构造的性质.

引理 2.1 令 $P(x,y)$ 是 Huff 曲线 E_{ab} 上的一点，方程 $f_{a,b}(s)=P$ 的解都是方程

$$\begin{aligned}&H_{a,b}(x,y):(ax-by)s^4+\\&2[3ab(bx-ay)-(ax-by)(a^2+b^2)]s^2+\\&6ab(a^2-b^2)s+(ax-by)[(a^2+b^2)^2-3a^2b^2]=0\end{aligned}$$

的解.

证明

$$\left.\begin{aligned}&ax(by^2-1)=by(ax^2-1)\\&H_{a,b}(x,y)=0\end{aligned}\right\}\Leftrightarrow$$

$$\left.\begin{aligned}&ax(by^2-1)=by(ax^2-1)\\&2s[(xs-b)ab^2-a^2b(ys-a)]=\\&\quad(ax-by)\left[a^2b^2-\frac{(a^2+b^2-s^2)^2}{3}\right]\end{aligned}\right\}\Leftrightarrow$$

$$\left.\begin{aligned}&ax(by^2-1)=by(ax^2-1)\\&(xs-b)ab^2-a^2b(ys-a)=(ax-by)v\end{aligned}\right\}\Leftrightarrow$$

$$\left.\begin{aligned}&ax(by^2-1)=by(ax^2-1)\\&\frac{xs-b}{ys-a}=\frac{a^2b-xv}{ab^2-yv}\end{aligned}\right\}\Leftrightarrow$$

$$\left.\begin{aligned}&(xs-b)u=a^2b-xv\\&(ys-a)u=ab^2-yv\end{aligned}\right\}\Leftrightarrow$$

$$\left.\begin{aligned}x&=\frac{b(u+a^2)}{su+v}\\y&=\frac{a(u+b^2)}{su+v}\end{aligned}\right\}.$$

由于 $H_{a,b}(x,y)$ 是关于 s 的 4 次方程，利用 Berlekamp 算法[21]，$f_{a,b}^{-1}(P)$ 是在多项式时间内可计算的，并且对于 Huff 曲线 E_{ab} 上的任意的点 $P(x,y)$，满足 $|f_{a,b}^{-1}(P)|\leqslant 4$.

3　构造到 Huff 曲线的散列函数

散列函数的单向性和抗碰撞性的定义如下：

定义 3.1　一个散列函数被称作是 (t,ϵ) 单向：任给一个 $y\in Im(h)$，$Im(h)$ 是象集，对于任意算法运行时间 t，输出 m，满足 $h(m)=y$ 的概率最多是 ϵ.

如果 ϵ 是可忽略的，则称 h 是单向的.

定义 3.2　一个散列函数簇 H 被称作是 (t,ϵ) 抗碰撞的：对于任意算法运行时间为 t，任给一个 $h\in H$，输出 (m,m') 满足 $m\neq m'$，$h(m)=h(m')$ 的概率最多是 ϵ. 如果 ϵ 是可忽略的，则称 H 是抗碰撞的.

下面证明当 h 是一个散列函数时，$H(m)=f_{ab}(h(m))$ 也是一个散列函数.

定理 3.1　如果函数 h 是 (t,ϵ) 单向的，可以证明 H 是 (t',ϵ') 单向的，其中 $\epsilon'=16\epsilon$.

证明　利用文献[16]中的引理 5，取 $L=4$ 直接得到.

定理 3.1 成立的原因是单向函数的象集中的元素，4 个映射成 1 个时，该单向函数依然是单向的.

定理 3.2　如果函数 $h:\{0,1\}^*\rightarrow\{0,1\}^k$ 是 (t,ϵ) 抗碰撞的，可以证明 H 是 (t',ϵ') 抗碰撞的，其中 $\epsilon'=\epsilon+\frac{2^{2k+2}}{q}$.

证明　利用文献[16]中的定理 3，取 $L=4$ 直接得到.

定理 3.2 成立的原因是单向函数的象集中的元素，4 个映射成 1 个时，该抗碰撞函数依然是抗碰撞的.

对于给定的散列函数簇 H，任意的 $h\in H$，定义函数 $H=f\circ h$，f 为 F_q 到 Huff 曲线上点的函数. H 中发生碰撞当且仅当：

（Ⅰ）存在 m 和 m'，使得 $h(m)=h(m')$，这是 h 的一个碰撞.

（Ⅱ）或者对于 $u=h(m)$，$u'=h(m')$，$u\neq u'$ 满足 $f(u)=f(u')$，这是 f 造成的一个碰撞.

在实际应用中，ϵ 一般为 $2^{-k/2}$. 如果 q 至少为 $\frac{5}{2}k$ 位，当 ϵ 是可忽略的，那么 $\epsilon'\leqslant 5\epsilon$ 也是可忽略的. 也就是说 h 是抗碰撞的，H 也是抗碰撞的.

这样就证明了当是一个散列函数时，H 也是一个散列函数.

4　算法效率分析

本文的实验选在 SM2 推荐的有限域 $F_{2^{256}-2^{224}-2^{96}+2^{64}-1}$ 上，大数运算库为 Miracl，CPU 为 Intel 酷睿 2 2.66 GHz，编译器为 Visual Studio 2008. 表 1 给出了实验数据，每个数据均运行 1 000 000次，取其平均值.

表 1　不同的域操作运行时间

Tab. 1　Time cost of different field operations

基础运算	时间/μs
求立方根 C	454.5
求逆 I	36.204
乘法 M、平方 S	1.721

在 f_{ab} 的表达式(式(2))中，a 和 b 是已知的，则 a^2，b^2 和 a^2b^2 可以预计算. F_q 中，$\frac{1}{3}$ 也是可以预计算的，则计算出 f_{ab} 需要 $2I+7M+3S+C$. 若 a,b 取，为较小的数，则只需要 $2I+5M+3S+C$. 因为求立方根是计算一个幂乘，所以计算 f_{ab} 的时间复杂性为 $O(\log^3 q)$.

利用文献[16]中的 Icart 函数加双有理等价的方法构造到 Huff 曲线的散列函数的花费为 $(I+2M+3S+C)+(2I+4M+2S)=3I+6M+5S+C$.

随机选择 a,b 时，实验计算 f_{ab} 的平均计算时间为 557.8 μs. 利用文献[16]中的 Icart 函数加双有理等价的方法构造到 Huff 曲线的散列函数的平均计算时间为 598.4 μs. 比较发现，本文算法比 Icart 函数加双有理等价的方法快 $I+M$. 实验数据快 $(598.4-557.8)/557.8=7.3\%$.

5　结论

本文首次构造了从有限域到 Huff 曲线的确定

函数,并且在此基础上构造了从字符串到 Huff 曲线的散列函数.在 SM2 推荐的有限域上,该散列函数的运行时间为 557.8 μs,比 Icart 函数加双有理等价的方法快 40.6 μs.该构造还为基于身份的协议的构造奠定了基础.

参考文献(References)

[1] Koblitz N. Elliptic curve cryptosystems [J]. Mathematics of Computation, 1987, 48(177): 203-209.

[2] Miller V S. Uses of elliptic curves in cryptography [C]// Proceedings of Advances in Cryptology-CRYPTO'85. Santa Barbara, USA: Springer, 1986: 417-428.

[3] Joye M, Tibouchi M, Vergnaud D. Huff's model for elliptic curves [C]// Lecture Notes in Computer Science. Brussels, Belgium: Springer-Verlag, 2010, 6234: 234-250.

[4] Devigne J, Joye M. Binary Huff curves[C]// Lecture Notes in Computer Science, CT-RSA. San Francisco, USA: Springer, 2011, 6558: 340-355.

[5] Elmegaard-Fessel L. Efficient scalar multiplication and security against power analysis in cryptosystemsbased on the nist elliptic curves over prime fields[EB/OL]. http://eprint.iacr.org/2006/313.

[6] Wu H F, Feng R Q. Elliptic curves in Huff's model [J]. Wuhan University Journal of Natural Sciences, 2012, 17(6): 473-480.

[7] Boneh D, Franklin M K. Identity-based encryption from the Weil pairing[C]// 21st Annual International Cryptology Conference. Santa Barbara, USA: Springer, 2001, 2139: 213-229.

[8] Horwitz J, Lynn B. Toward hierarchical identity-based encryption[C]// Lecture Notes in Computer Science, Amsterdam, Netherlands: Springer, 2002, 2332: 466-481.

[9] Boneh D, Gentry C, Lynn B, et al. Aggregate and verifiably encrypted signatures from bilinear maps [C]// International Conference on the Theory and Applications of Cryptographic Techniques. Warsaw, Poland: Springer, 2003, 2656: 416-432.

[10] Cha J C, Cheon J H. An identity-based signature from gap Diffie-Hellman groups [C]// Proceedings of 6th International Workshop on Practice and Theory in Public Key Cryptography. Miami, USA: Springer, 2003, 2567: 18-30.

[11] Zhang F G, Kim K. Id-based blind signature and ring signature from pairings [C]// Proceedings of 8th International Conference on the Theory and Application of Cryptology and Information Security. Queenstown, New Zealand: Springer, 2002: 533-547.

[12] Boyen X. Multipurpose identity-based signcryption: A Swiss army knife for identity-based cryptography[C]// Proceedings of the 23rd International Conference on Advances in Cryptology. Santa Barbara, USA: Springer, 2003: 383-399.

[13] Libert B, Quisquater J J. Efficient signcryption with key privacy from gap Diffie-Hellman groups [C]// Proceedings of 7th International Workshop on Theory and Practice in Public Key Cryptography. Singapore: Springer, 2004: 187-200.

[14] Lindell Y. Highly-efficient universally-composable commitments based on the DDH assumption[C]// 30th Annual International Conference on the Theory and Applications of Cryptographic Techniques. Tallinn, Estonia: Springer, 2011: 446-466.

[15] Shallue A, van de Woestijne C E. Construction of rational points on elliptic curves over finite fields[C]// Proceedings of 7th International Symposium. Berlin, Germany: Springer, 2006: 510-524.

[16] Icart T. How to hash into elliptic curves[C]// 29th Annual International Cryptology Conference. Santa Barbara, USA: Springer, 2009: 303-316.

[17] Brier E, Coron J S, Icart T, et al. Efficient indifferentiable hashing into ordinary elliptic curves [C]// Proceedings of 30th Annual Cryptology Conference. Santa Barbara, USA: Springer, 2010: 237-254.

[18] Farashahi R R, Fouque P A, Shparlinski I E, et al. Indifferentiable deterministic hashing to elliptic and hyperelliptic curves[J]. Mathematics of Computation, 2013, 82(281): 491-512.

[19] Farashahi R R. Hashing into Hessian curves [C]// Lecture Notes in Computer Science. Dakar, Senegal: Springer, 2011: 278-289.

[20] Yu W, Wang K, Li B, et al. About hash into Montgomery form elliptic curves[C]// Proceedings of the 9th International Conference on Information Security Practice and Experience. Lanzhou, China: Springer, 2013: 147-159.

[21] Shoup V. A new polynomial factorization algorithm and its implementation [J]. Journal of Symbolic Computation, 1995, 20(4): 363-397.