УДК 511.6

А. В. Пузаков

ЭФФЕКТИВНЫЕ АЛГОРИТМЫ ВЫЧИСЛЕНИЙ НА СУПЕРЭЛЛИПТИЧЕСКИХ КРИВЫХ

Представлены базовые алгоритмы арифметики суперэллиптических кривых и оптимальные параметры суперэллиптических кривых пригодных для криптографии.

Represents basics algorithms of arithmetics superelliptic curves and optimal parameters superelliptic curve suitable for cryptography.

Ключевые слова: криптография, алгебраические кривые, суперэллиптические кривые, функциональные поля.

Key words: cryptography, algebraic curves, superelliptic curves, functional fields.

Современная криптография — это баланс между стойкостью и быстродействием при минимальных затратах памяти. Такие ограничения в первую очередь вводят чипированные банковские карты [1]. Больших успехов на этом направлении добилась криптография с открытым ключом основанная на эллиптической кривой ANSI X9.62 и X9.63 [2].

В 2000 году [3] был предложен новый тип кривых вида

$$C : y^n = c(x). \tag{1}$$

Такой вид кривых называют *суперэллиптическими*.

Развитие алгебры суперэллиптических кривых обусловлено большой степени свободы при задании кривой. Необходимо вычислять дивизоры точек и якобиан, а также иметь хорошее представление идеалов. Все это — мощный инструмент для разработки криптосистем. К сожалению, на сегодня практическая реализация криптосистемы на СЭК отсутствует, в печати даются лишь теоретические оценки, что свидетельствует о недостаточной разработке данного направления [5].

Суперэллиптические кривые обладают набором свойств [2]: 1. C не сингулярная аффинная кривая. 2. Существует только одна точка P_∞. 3. Род кривой C $0{,}5(\nu-1)(\delta-1)$. 4. Целое замыкание $k[x]$ в функциональном поле $k(C)$ $O := \kappa[\xi,\psi]/\left(\psi^{\nu}-\chi(\xi)\right)$.

Хорошо известен факт из теории дедекиндовых колец, что любой целый идеал $K[C]$ порождается полиномом из $K[\Xi]$ и вторым полиномом из $K[X]$. Таким образом, любой редуцированный K-рациональный дивизор D можно записать в виде $\Delta = \delta\iota\varpi\left(\upsilon,\rho\Psi^2+\sigma\Psi+\tau\right)$, где $\upsilon,\rho,\sigma,\tau\in K[\xi]$, $\delta\varepsilon\gamma\rho,\ \delta\varepsilon\gamma\sigma,\ \delta\varepsilon\gamma\tau < \delta\varepsilon\gamma\rho \le \gamma,\ \gamma\chi\delta(\upsilon,\rho,\sigma,\tau)=1$.

Согласно [4] между главными дивизорами P из C и главными идеалами $\mathfrak{p}$ из $K[\xi]$ существует взаимно-однозначное соответствие — гомоморфизм: $\sum m_p P \leftrightarrow \prod \mathfrak{p}^{m_p}$, $\delta\iota\varpi(\alpha_1,\ldots,\alpha_\nu) \leftrightarrow \alpha_1,\ldots,\alpha_\nu$

Всякий полуредуцированный дивизор D может быть записан в виде $D = \sum m_i(u_i, v_i) - (\sum m_i)_\infty = \text{НОД}(\operatorname{div} a(x), \operatorname{div}(b(x)-y)) = \langle u, Y - v\rangle$ главных дивизоров $\operatorname{div} a(x) u \operatorname{div}(b(x)-y)$, где $a(x)$ и $b(x)$ — многочлены, $a(x) = \prod (x-u_i)^{m_i}$. В гиперэллиптических кривых для каждой точки $P_i = (u_i, v_i)$ существует единственный многочлен $b_i \in K[x]$, удовлетворяющий 1) $\deg b_i < m_i$; 2) $b_i(u_i) = v_i$; 3) $(x-u_i)^{m_i} \mid b_i^2(x) + b_i(x)h(x) - f(x)$.

Для ускорения вычислений используем рекуррентную процедуру вычисления многочленов. Если $P_i = (u_i, v_i)$ — специальная точка, то $b_k(x) = v_i$. Если $P_i = (u_i, v_i)$ — обыкновенная, то $b_i(x)$ ищем в виде $b_i(x) = c_0 + c_1(x-u) + c_2(x-u)^2 + \ldots + c_{k-1}(x-u)^{k-1}$, где $k = m_i$, $c_0 = b_i(u_i) = v_i$.

Обозначим $t = x - u_i$. Тогда $x = t + u_i$. Положим, $\eta(t) = h(t+u_i)$, $\varphi(t) = f(t+u_i)$ и $\beta_i(t) = b_k(t+u_i)$. Тогда $\beta_i(t) = c_0 + c_1 t + c_2 t^2 + \ldots + c_{k-1}t^{k-1}$ и из 3) следует $\beta_i^2(t) + \beta_i(t)\eta(t) \equiv \varphi(t) \left(\operatorname{mod} t^k\right)$. Для $c_0, c_1, c_2, \ldots c_{k-1}$:

$$c_1 = \frac{\varphi_1 - \eta_1 c_0}{2c_0 + \eta_0},\ c_2 = \frac{\varphi_2 - \eta_1 c_1 - \eta_2 c_0 - c_1^2}{2c_0 + \eta_0},\ c_3 = \frac{\varphi_3 - \eta_1 c_2 - \eta_2 c_1 - \eta_3 c_0 - 2c_1 c_2}{2c_0 + \eta_0},$$

$$\chi_4 = \frac{\varphi_4 - \eta_1\chi_3 - \eta_2\chi_2 - \eta_3\chi_1 - \eta_4\chi_0 - 2\chi_1\chi_3 - \chi_2^2}{2\chi_0 + \eta_0},$$

при $j > 4$, c_j считаются равными

$$c_4 = \frac{\varphi_j - \eta_1 c_{j-1} - \eta_2 c_{j-2} - \ldots - \eta_j c_0 - c_1 c_{j-1} - c_2 c_{j-2} - \ldots - c_{j-2}c_2 - c_{j-1}c_1}{2c_0 + \eta_0},$$

где $j \le k-1$. Подробнее с процедурой можно ознакомиться в статье [7].

Для суперэллиптической кривой приведенная процедура так же верна, но с рядом ограничений. Если $h(x) = 0$, то используем пункт 3): $(x-u_i)^{m_i} \mid b_i^n(x) - f(x)$, следовательно, $\beta_i^n(t) \equiv \varphi(t) (\operatorname{mod} t^k)$.

Для использования суперэллиптических кривых для цифровой криптографии необходимо, чтобы они обладали дополнительными свойствами. Для современных систем наибольший интерес представляют криптосистемы, имеющие хорошие показатели над полями с любой характеристикой. Если $h(x) = 0$, то $\eta(t) = 0$, откуда следует, что для кривой рода 2 и характеристикой поля 2 использование рекуррентной формулы не представляется возможным. Отсутствие эффективного алгоритма вычисления дивизоров $\operatorname{div} a(x)$ и $\operatorname{div}(b(x)-y)$ делает использование суперэллиптических кривых рода 2 невозможным. Это означает, что оптимально использовать кривые рода 3 и 4.

Определение походящих точек $P_i = (u_i, v_i)$ можно ускорить использованием $c(x)$ вида $Ax^n + Bx^{n-k} + C$. Большое количество нулевых коэффициентов сократит время поиска точек. (1) можно переписать в виде $C: y^n = Ax^m + Bx^{m-k} + C$, где $n \in \{3,4\}$, $n \le m$, $k \in \{1,2,\ldots,m-1\}$.

Необходимо определить базовые арифметические операции над идеалами над суперэллиптическими кривыми.

Как и в гиперэллиптических кривых, произведение двух идеалов $\alpha_1 = \langle u_1, Y - v_1 \rangle$ и $\alpha_2 = \langle u_2, Y - v_2 \rangle$ проходит в два шага. На первом этапе вычисляется произведение $\alpha_1\alpha_2 = \langle u, Y - v \rangle$, на втором — полученный идеал степени $2g$ редуцируется до степени не превышающую g.

Если $\alpha_1 = \langle u_1, Y - v_1 \rangle$ и $\alpha_2 = \langle u_2, Y - v_2 \rangle$ — редуцированные идеалы в $K[C]$, $u_i, v_i \in K[x]$, $\deg v_i < \deg u_i \le g$ и $v_i^3 - f = u_i w_i$ для некоторого $w_i \in K[x]$ предположим, что $\text{НОД}\left(\upsilon_1, \upsilon_2, \varpi_1^2 + \varpi_1\varpi_2 + \varpi_2^2\right) = 1$ и $s_1, s_2, s_3 \in K[X]$ такие, что $s_1u_1 + s_2u_2 + s_3\left(v_1^2 + v_1v_2 + v_2^2\right) = 1$.

Если $u = u_1u_2$, $\underline{v} = v_1 + s_1u_1(v_2 - v_1) - s_3(v_1^3 - f)$, $v = \underline{v} \bmod u$ и $\alpha = \langle u, Y - v \rangle$, то $\alpha_1\alpha_2 = \alpha$ и $u \mid v^3 - f$.

1. Возведение в степень. Пусть $\alpha_1 = \langle u_1, Y - v_1 \rangle$ — редуцированный идеал и $v_i^3 - f = u_i w_i$. Если $\text{НОД}(u_1, v_1) = 1$, то $s_1u_1 + 3s_3v_1^2 = 1$.

Если $u = u_1^2$, $t = -s_3w_1 \bmod u_1$, $v = v_1 + tu_1$, то $\alpha_1^2 = u, Y - v$.

2. Произведение. Если $\alpha_1 = \langle u_1, Y - v_1 \rangle$, $\alpha_2 = \langle u_2, Y - v_2 \rangle$ — идеалы и $v_i^3 - f = u_i w_i$, $\text{НОД}(u_1, u_2) = 1$, то $s_1u_1 + s_2u_2 = 1$.

Если $u = u_1u_2$, $t = s_1(v_2 - v_1) \bmod u_2$, $v = v_1 + tu_1$, то $\alpha_1\alpha_2 = u, Y - v$.

3. Инвертирование. Если $\alpha = <u, Y - v>$ редуцированный идеал и $v^3 - f = uw$, $\text{НОД}(u, w) = 1$, то $\langle u \rangle \alpha^{-1} = \left\langle u, Y^2 + uY + u^2 \right\rangle$.

4. Редуцирование. Вход: идеал α из $K[C]$.

Выход: редуцированный идеал $\text{Re}\,d(\alpha)$ эквивалентный α.

1) Выберем идеал β из α^{-1} такой, что $\beta = \alpha^{-1}$ для некоторого $u \in \alpha$.

2) Пусть $e \ne 0$ — минимальный.

3) $\text{Re}\,d(\alpha) = eb^{-1} = \frac{e}{u}\alpha$.

Доказательства приведенных алгоритмов можно посмотреть в [4].

Заключение

Полученные результаты дают возможность программной реализации вычислений якобиана суперэллиптических кривых, позволяющей определить реальные перспективы использования суперэллиптических кривых для криптографии. Остаются вопросы выбора подходящий точек и определения криптографических свойств получаемых якобианов.

В случае успешной реализации криптография на суперэллиптических кривых сможет заменить эллиптические кривые в криптосистемах с открытым ключом и в системах электронных цифровых подписей.

Список литературы

1. *Koblitz N.* Elliptic curve cryptosystems // Mathematics of Computation. 1987. № 48 (177). P. 203–209.

2. *ANSI X9.63* Public Key Cryptography for the Financial Services Industry: Elliptic Curve Key Agreement and Key Transport Schemes. Working Draft - Version 2.0. 1998.

3. *Galbraith S.D., Paulus S.M., Smart N.P.* HPL-98-179, 1998.

4. *Basiri A., Enge A., Faugere J.C., Gurel N.* // Mathematics of Computation. 1998. № 74 (249). P. 389–410.

5. *Galbraith S.D., Paulus S.M., Smart N.P.* // Mathematics of Computation. 2002. № 71 (237). P. 393–405.

6. *Ковтун В.Ю.* Криптография с открытым ключом. URL: http://www.nrjetix.com/fileadmin/doc/publications/additional_info/public_key_cryptography_-_lecture.pdf (дата обращения: 10.07.2015).

7. *Алешников С.И.* Рекуррентная процедура вычисления представляющих многочленов в алгоритме шифрования, основанном на гиперэллиптических кривых // Вестник Российского государственного университете им. И. Канта. 2007. Вып. 10. С. 65—69.

Об авторе

Александр Васильевич Пузаков — асп., Балтийский федеральный университет им. И. Канта, Калининград.

E-mail: apuzakov@kantiana.ru

About the author

Alexandr Puzakov — PhD student, I. Kant Baltic Federal University, Kaliningrad.

E-mail: apuzakov@kantiana.ru