XXXII Неделя науки СПбГПУ. Материалы межвузовской научно-технической конференции. Ч.V : С.167-168

СЕКЦИЯ «ИНФОРМАЦИОННАЯ БЕЗОПАСНОСТЬ КОМПЬЮТЕРНЫХ СИСТЕМ»

УДК 50.41.00

О.В.Шемякина (3 курс, каф. ИБКС), А.Г.Ростовцев, д.т.н., проф.

РАЗЛОЖЕНИЕ ПРОСТОГО ЧИСЛА В $Z[\sqrt{-D}]$

Рассматривается алгоритм Полларда и Шнорра применительно к разложению простого числа в неевклидовых мнимых квадратичных порядках $Z[\sqrt{-3}]$, $Z[\sqrt{-4}]$, $Z[\sqrt{-7}]$, $Z\left[\frac{1+\sqrt{-19}}{2}\right]$, $Z\left[\frac{1+\sqrt{-27}}{2}\right]$ $Z\left[\frac{1+\sqrt{-43}}{2}\right]$, $Z\left[\frac{1+\sqrt{-67}}{2}\right]$, $Z\left[\frac{1+\sqrt{-163}}{2}\right]$, которые определяют комплексное умножение на соответствующей эллиптической кривой над $\Re$. Показано, что алгоритм корректен и при условии $\left(\frac{-D}{p}\right)=1$ выдает единственно представление простого числа p или $4p$ в виде суммы $a^2 + Db^2$. Это представление может быть использовано при быстрой генерации эллиптических кривых с хорошими криптографическими свойствами.

Эллиптическая кривая $E(K)$ над полем K характеристики, отличной от 2, 3, задается уравнением $y^2 = x^3 + Ax + B$, где полином в правой части не имеет кратных корней в K. Инвариант эллиптической кривой равен $j=\frac{12^3 4A^3}{4A^3+27B^2}$. Эллиптическая кривая задается своим j-инвариантом с точностью до изоморфизма.

Эллиптические кривые над конечными полями являются наиболее перспективной и наиболее популярной математической структурой для построения криптографических алгоритмов. На эллиптических кривых строится отечественный ГОСТ Р 34.10–2001 и американский ECDSS стандарты электронной подписи. Эллиптические кривые позволяют реализовать широкий спектр криптографических протоколов.

Для выбора параметров криптосистемы необходимо уметь рассчитывать число точек эллиптической кривой. Для расчета числа точек кривой $E(\oplus_p)$ требуется найти представление $p=(a+b\sqrt{-D})(a-b\sqrt{-D})=a^2+Db^2$ или при $D \equiv 3 \pmod 4$.

$$p=\left(a+b\frac{1+\sqrt{-D}}{2}\right)\left(a+b\frac{1-\sqrt{-D}}{2}\right)=a^2+ab+b^2\frac{D+1}{4}.$$

Алгоритм разложения характеристики поля в мнимом квадратичном порядке был предложен Поллардом и Шнорром. Он по сути представляет собой расширенный алгоритм Евклида в мнимом квадратичном порядке $Z[\sqrt{-D}]$. Ситуация осложняется тем, что некоторые порядки не являются евклидовыми (то есть алгоритм Евклида в этих кольцах не работает). В данной работе была предложена модификация этого алгоритма для рассматриваемых мнимых квадратичных порядков. В результате были доказаны следующие теоремы.

Теорема 1. Для того чтобы искомое разложение существовало, необходимо чтобы

выполнялось условие $\left(\frac{-D}{p}\right)=1$. Если такое разложение существует, то оно единственно за исключением случая $Z[\sqrt{-3}]$, когда для числа 4*p* существуют два разложения.

Теорема 2. Разложение простого числа $p \in \wedge$ на простые множители в виде произведения целых квадратичных чисел

$$p=(a+b\sqrt{-D})(a-b\sqrt{-D})=a^2+Db^2$$

при $-D = -1, -2, -3$ и

$$4p=(a+b\sqrt{-D})(a-b\sqrt{-D})=a^2+Db^2$$

при $-D = -7, -11, -19, -43, -67, -163$ в главных квадратичных порядках возможно тогда и только тогда, когда $\left(\frac{-D}{p}\right)=1$.

Теорема 3. Для рассматриваемых квадратичных порядков предложенный алгоритм корректен.

Таким образом, предложенный алгоритм может быть использован для быстрой генерации эллиптических кривых и построения надежных и эффективных криптосистем.