УДК 004.056.55

П. С. Захаров[1], *М. Г. Пискун*[2]

[1]Московский физико-технический институт (государственный университет)

Представления точек на эллиптических кривых

В современных информационных системах большое значение имеет криптография с открытым ключом. Подобные системы реализованы, к примеру на эллиптических кривых. Они используют проблему дискретного логарфима в применении к точкам на эллиптических кривых над конечными полями. Подобные системы нашли применение, к примеру, в ГОСТ Р 34.10-2012. В практических применениях важна не только защищенность системы, но и ее производительность. Различные представления точек на кривых позволяют оптимизировать процесс вычислений и ускорить производительность. В данной статье рассматриваются различные представления точек с точки зрения количества требуемых операций и используемой памяти на примере ECDSA - алгоритма для создания цифровой подписи.

Ключевые слова: Криптография с открытым ключом, эллиптические кривые, ЭЦП

1. Введение

В настоящее время распространены ассиметричные криптографические алгоритмы с открытым ключом. В таких алгоритмах существует два ключа - открытый, передавемый по незащищенному каналу, и закрытый, держащийся в тайне и тяжело вычисляющийся из открытого. Такие системы используются для проверки цифровых подписей или обмена ключами от симметричных систем. К ним относятся широко известные алгоритмы Диффи-Хеллмана, Эль-Гамаля, шифр RSA и другие.

Реалии современного мира предъявляют высокие требования как к защищенности криптосистем, так и к их производительности. Первое требование, помимо прочего, обуславливает выбор больших параметров системы (к примеру, порядку используемого конечного поля), в особенности для ассиметричных криптосистем. В сочетании с большим количеством вычислений, требующихся для произведения одной итерации шифрования или создания одной подписи, это явно противоречит второму требованию. В связи с этим используются различные методики более быстрых вычислений.

В криптографии на эллиптических кривых основой вычислений являются операции над точками на кривой - сложение и умножение на число. Каждая из этих операций подразумевает определенное количество сложений, умножений и инверсий в конечном поле. Более сложные представления точек позволяют сократить число этих операций за счет хранения большего числа информации. В данной работе сравниваются разные представления с точки зрения производительности и используемой памяти. В разделе 1 вводятся эллиптические кривые, в разделе 2 описывается тестовый алгоритм - <алгоритм>, в разделе 3 - вычислительный эксперимент. В разделе 4 обсуждаются результаты.

2. Название 1го раздела

Текст первого раздела.

3. Название 2го раздела

Текст второго раздела.

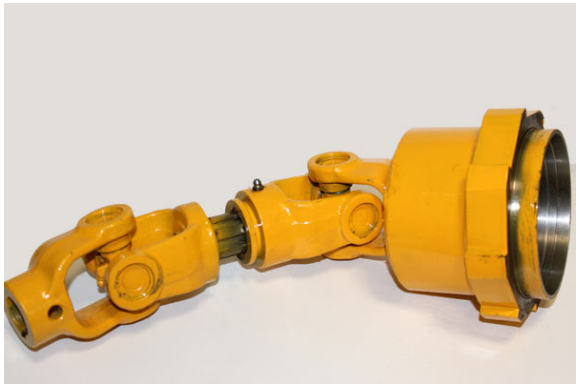

Рис. 1. Пример вставки рисунка

а) б)

Рис. 2. Пример вставки двух рисунков в одну строчку с общей подписью

4. Название 3го раздела

Текст третьего раздела. Пример формулы с нумерацией:

$$\lim_{x\to 0}\frac{\sin x}{x}=1. \tag{1}$$

Пример формулы без нумерации:

$$\lim_{x\to\infty}\left(1+\frac{1}{x}\right)^x=e,$$

где e — экспонента. Пример ссылки на литературу [1].

4.1. Название подраздела 3.1

Текст подраздела 3.1. Пример ссылки на формулу (1).

4.2. Название подраздела 3.2

Текст подраздела 3.2. Пример таблицы.

5. Заключение

Текст заключения.

Работа выполнена при поддержке Минобрнауки, проект № 10А.100.

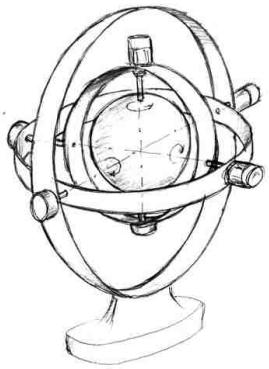

Рис. 3. Пример вставки двух рисунков в одну строчку — первый рисунок

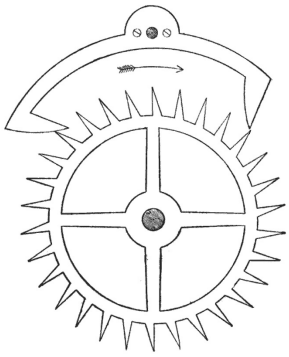

Рис. 4. Два рисунка в одну строчку — второй рисунок

Таблица 1

Название таблицы

		Столбец 1	Столбец 2
Строка 1	Строка 1.1	Ячейка 1	Ячейка 2
	Строка 1.2	Ячейка 3	Ячейка 4
Строка 2	Строка 2.1	Ячейка 5	Ячейка 6
	Строка 2.2	Ячейка 7	Ячейка 8

Литература

1. *Шевченко Д. В., Шевченко В. П.* Выбор и оптимизация структуры построения автономных сейсмических средств обнаружения рубежного типа // Материалы VIII всероссийской научно-технической конференции «Современные охранные технологии и средства обеспечения комплексной безопасности объектов». — 2010. — С. 128–133.
2. *Diallo M. S., Kulesh M., Holschneider M., Sherbaum F., Adler F.* Characterization of polarization attributes of seismic waves using continuous wavelet transforms // Geophysics. — 2006. — V. 71, N. 3. — P. 67–77.
3. *Лайонс Р.* Цифровая обработка сигналов. — М.: Бином, 2006. — С. 361–369.

References

1. *Shevchenko D. V., Shevchenko V. P.* Selection and optimization of constructing autonomous seismic detection struction a landmark type // Proceedings of the VIII Russian scientific conference “Modern security technology and means of complex security objectives”. — 2010. — P. 128–133. — (in Russian).
2. *Diallo M. S., Kulesh M., Holschneider M., Sherbaum F., Adler F.* Characterization of polarization attributes of seismic waves using continuous wavelet transforms // Geophysics. — 2006. — V. 71, N. 3. — P. 67–77.
3. *Lyons R.* Digital signal processing. — M.: Binom, 2006. — P. 361–369. — (in Russian).

Поступила в редакцию дд.мм.гггг.