АЛГОРИТМЫ СОКРАЩЕНИЯ БАЗИСА РЕШЕТКИ В КРИПТОАНАЛИЗЕ

Черниш Д. И.
Научный руководитель – к.т.н., доц. Мельникова О. А.
Харьковский национальный университет радиоэлектроники (61166, Харьков, пр. Науки,14, каф. Безопасности информационных технологий, тел. (057) 702-14-25), e-mail: denys.chernysh@nure.ua

Reducing the basis of the lattice is a fundamental tool in cryptanalysis and is used to successfully attack many cryptosystems based on both lattices and other mathematical problems. The success of lattice methods in cryptanalysis is largely specified reduction algorithms work much better in practice than their theoretical worst-case analysis predicts. Over the past 30 years, basic reduction algorithms have been studied in many works, but the gap between theoretical analysis and practical efficiency is still largely inexplicable.

Сокращение базиса решетки является фундаментальным инструментом в криптоанализе и используется для успешной атаки на многие криптосистемы, основанные как на решетках, так и на других математических задачах. Успех решеточных методов в криптоанализе в значительной степени обусловлен тем фактом, что алгоритмы редукции на практике работают намного лучше, чем предсказывает их теоретический анализ наихудшего случая. За последние 30 лет алгоритмы базисной редукции исследовались во многих работах, но разрыв между теоретическим анализом и практической эффективностью все еще в значительной степени необъясним. Этот пробел препятствует способности оценивать безопасность криптографических функций на основе решетки, и он широко признан в качестве одного из основных препятствий на пути использования решеточной криптографии на практике.

По большому счету, современное состояние редукции базиса решетки (в теории и на практике) представлено двумя алгоритмами:

1) практичный алгоритм Шнорра и Эйхнера Block-Korkine-Zolotarev (BKZ) в его современном воплощении BKZ 2.0, включающий в себя стратегии обрезки, рекурсивной предварительной обработки и раннего завершения;

2) алгоритм уменьшения Slide Гамы и Нгуена, элегантное обобщение LLL [1], которое доказуемо аппроксимирует короткие векторы решетки в пределах факторов, связанных с неравенством Морделла.

Оба алгоритма используют оракул кратчайшей векторной задачи (SVP) для решеток малого размера, которые параметризованы границей k (называемой «размером блока») на размерности этих решеток. Алгоритм сокращения Slide имеет много привлекательных особенностей: он делает только полиномиальное количество вызовов оракула SVP, все вызовы SVP относятся к спроецированным подрешеткам в том же измерении k, а также он достигает наилучшей известной верхней границы наихудшего случая

для длины его кратчайшего выходного вектора: $\gamma_k^{(n-1)/(2(k-1))}\det(L)^{1/n}$, где $\gamma_k = \Theta(k)$ – постоянная Эрмита, а $\det(L)$ – определитель решетки. К сожалению, сообщалось, что в экспериментах алгоритм BKZ превосходит алгоритм уменьшения Slide, BKZ дает гораздо более короткие векторы для сопоставимого размера блока. Фактически, отмечается, что даже BKZ с размером блока $k = 20$ дает лучшие уменьшенные базы, чем уменьшение Slide с размером блока $k = 50$. Как следствие, алгоритм уменьшения Slide никогда не используется на практике, а также он не был реализован и экспериментально проверен.

С другой стороны, хотя алгоритм BKZ удивительно практичен в экспериментальных оценках, он также имеет свои недостатки. В первоначальном виде для BKZ даже не известно, что он завершается после полиномиального числа обращений к оракулу SVP, и сообщается, что его наблюдаемое время выполнения полиномиально растет, даже когда размер блока установлен на некоторое относительно малое значение $k \approx 30$. Даже после завершения наилучшие доказуемые границы качества вывода BKZ хуже, чем уменьшение Slide, по крайней мере, на полиномиальный коэффициент [1].

Алгоритм уменьшения Slide является гораздо более практичным, чем первоначально предполагалось авторами и, по мере увеличения размера он работает почти так же хорошо, как BKZ, но в то же время предлагает простую замкнутую формулу для оценки качества выхода. Это обеспечивает простой и эффективный метод оценки воздействия атак с уменьшением базиса решетки на решеточную криптографию без необходимости запуска симуляторов или других компьютерных программ [2]. Ключом к данным выводам является процедура перечисления кратчайших векторов решетки в двойных решетках без необходимости явного вычисления двойного базиса. Процедура двойного перечисления почти идентична (синтаксически) стандартной процедуре перечисления для поиска коротких векторов в первичной решетке, и она столь же эффективна на практике.

Список использованных источников:

1. A.K. Lenstra, H.W. Lenstra, Jr. and L. Lov´asz. Factoring polynomials with rational coefficients. Mathematische Annalen, 261:513–534, 1982.

2. M. Albrecht, D. Cad´e, X. Pujol, and D. Stehl´e. fplll-4.0, a floating-point LLL implementation. Available at http://perso.ens-lyon.fr/damien.stehle.