2022, Volume 9, Number 2
http://www.jcomsec.org

Journal of Computing and Security

طراحی الگوریتم BKZ ـ پیشرونده بهینه با احتمال‌های موفقیت افزایشی و اندازه بلوک‌های افزایشی

Persian Abstract

غلامرضا مغیثی [آ]، علی پاینده [آ,*]

[آ] دپارتمان ICT، دانشگاه صنعتی مالک اشتر تهران، تهران، ایران

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 2 October 2021
اصلاح: 27 November 2022
پذیرش: 12 December 2022
انتشار آنلاین: 28 February 2023

کلمات کلیدی:
BKZ پیشرونده بهینه، اندازه بلوک افزایشی، احتمال موفقیت افزایشی، هزینه زمانی، بازشماری GNR.

چکیده

مطالعات گذشته روی الگوریتم BKZ ـ پیشرونده غالبا تمرکز بر روی افزایش اندازه بلوک‌ها داشته است. مقاله‌ای از نویسندگان، منتشر شده در IJCNIS ۹.۹، ۲۰۱۸، یک نسخه‌ی جدید از الگوریتم BKZ ـ پیشرونده مبتنی بر افزایش احتمال‌های موفقیت را ارائه نمود که نتایج حاصل از آن به اندازه کافی امیدبخش نبوده است! این مقاله دو الگوریتم "BKZ با اندازه بلوک‌های افزایشی بهینه" و "BKZ با احتمال‌های موفقیت افزایشی بهینه" را ارائه می‌کند به‌طوریکه اثبات می‌شود پیچیدگی زمانی آنها بهینه است. هرچند این دو الگوریتم پیشنهادی جهت حل مسئله exact-SVP روی پایه مشبکه ورودی طراحی شده است، ولی می‌توان از آنها به عنوان حل کننده‌ـ SVP در بدنه یک الگوریتم BKZ دیگر برای حملات مشبکه در عمل نیز استفاده نمود! همچنین برای اولین بار در این مقاله، از این دو الگوریتم پیشنهادی به عنوان نمایندگانی معقول و مناسب از رویکردهای "اندازه‌های بلوک افزایشی" و "احتمال‌های موفقیت افزایشی" در خانواده الگوریتم‌های ـ پیشرونده، جهت مقایسه این دو رویکرد استفاده شد. در ابعاد پایه مشبکه $n \geq 90$، نتایج این مقاله زمان اجرای بهتری را برای "الگوریتم BKZ با احتمالهای موفقیت افزایشی بهینه" نسبت به نمونه‌های متناظر در "الگوریتم BKZ با اندازه بلوک‌های افزایشی بهینه" نشان داده است به طوریکه برای چالش‌های مشبکه Gentry-Halevi، این تسریع زمانی عبارتست از: "تسریع زمانی $2^{14.1}$ برابری برای چالش‌های غیرجدی با ابعاد مشبکه n=512"، "تسریع زمانی $2^{67.2}$ برابری برای چالش‌های کوچک با ابعاد مشبکه n=2048"، "تسریع زمانی $2^{235.5}$ برابری برای چالش‌های متوسط با ابعاد مشبکه n=8192" و "تسریع زمانی $2^{1207.7}$ برابری برای چالش‌های بزرگ با ابعاد مشبکه n=32768". همچنین در ابعاد مشبکه $100 \leq \beta \leq 240$، هزینه زمانی "الگوریتم BKZ با احتمال‌های موفقیت افزایشی بهینه" و "الگوریتم BKZ با اندازه بلوک‌های افزایشی بهینه" به عنوان دو حل‌ـ کننده مسئله exact-SVP، با تعدادی از الگوریتم‌های مدعی اصلی جهت حل مسئله exact-SVP از قبیل الگوریتم غربال (Sieve)، الگوریتم بازشماری هرس مفرط (extreme-pruned enumeration)، تابع بازشماری کامل (full-enumeration) و غیره، مقایسه شده و نتایج حاصل از این مقایسه، نشان دهنده زمان اجرای امیدبخشی برای الگوریتم‌های پیشنهادی ما بوده است. درنهایت، مدل زمانی (Cost-Model) برای دو الگوریتم پیشنهادی BKZ ـ پیشرونده در این مقاله تقریب زده شد.

* نویسنده مسئول.
آدرس‌های رایانامه: fumoghissi@chmail.ir (غ. مغیثی)،
payandeh@mut.ac.ir (ع. پاینده)

ISSN: 2322-4460