Research Article, 2021, Volume 8, Number 1
http://www.jcomsec.org

Journal of Computing and Security

رد سرعت ادعا شده در هرس مفرط و اصلاح BKZ 2.0 برای سرعت بیشتر

غلامرضا مقیسی [آ]، علی پاینده [آ،*]

[آ] گروه فناوری اطلاعات و ارتباطات ، دانشگاه صنعتی مالک اشتر ، تهران ، ایران.

اطلاعات مقاله

تاریخچه مقاله:
دریافت: 20 January 2021
اصلاح: 31 May 2021
پذیرش: 14 July 2021
انتشار آنلاین: 7 September 2021

کلمات کلیدی:
هرس مفرط، تابع بازشماری GNR، تسریع هزینه، الگوریتم BKZ 2.0، الگوریتم BKZ-revised.

چکیده

الگوریتم BKZ 2.0 یکی از الگوریتم‌های کاهش مشبکه‌ی مدعی می‌باشد که هرس مفرط به عنوان فاز اصلی آن محسوب می‌شود. هرس مفرط و هرس غیرمفرط (به ترتیب) در اولین مقاله‌ی مربوطه از گاما-ناین-ریجیو (سال ۲۰۱۰) مدعی دستیابی به حداکثر تسریع زمانی $۲^{\beta/۲}$ و $۲^{\beta/۴}$ نسبت به بازشماری کامل (بدون هرس) شدند. برای اندازه‌ی بلوک $\beta \leq ۳۷$، این مقاله تسریع زمانی مورد ادعای $۲^{\beta/۴}$، بوسیله‌ی یک بازشماری هرس شده‌ی غیرمفرط با تابع تحدید بهینه را تایید نموده است، درحالی‌که برای اندازه‌های بلوک در کاربردهای عملی شامل $۲۵۰ \leq \beta \leq ۱۰۰$، زمانی که بلوک مفروض بوسیله‌ی BKZ با تابع بازشماری پیش‌پردازش شود، مقدار حد بالای تسریع زمانی بازشماری با هرس مفرط (روی آن بلوک) در بازه‌ی $۲^{\beta/۶.۶}$ تا $۲^{\beta/۴.۴}$ تخمین زده می‌شود و زمانی که بلوک مفروض بوسیله‌ی BKZ با تابع غربال پیش‌پردازش شود مقدار حد بالای این تسریع زمانی در بازه‌ی $۲^{\beta/۹.۸}$ تا $۲^{\beta/۳.۴}$ تخمین زده می‌گردد. با دستیابی به این حد بالا برای تسریع زمانی حاصل از هرس مفرط، تمامی تحلیل‌های امنیتی که تاکنون از فرض تسریع $۲^{\beta/۲}$استفاده نموده‌اند باید بازبینی یا حتی در صورت لزوم رد شوند! همچنین این مقاله یک نسخه‌ی بازبینی شده از BKZ 2.0 را ارائه می‌نماید که برای ابعاد بلوک در کاربردهای عملی شامل $۲۵۰ \leq \beta \leq ۱۰۰$ و تعداد دورهای اصلی $\mathcal{N} \approx \infty$ از BKZ، مقدار حد پایین تسریع زمانی آن نسبت به BKZ 2.0 بوسیله‌ی فاکتور $\rho_۰$ تخمین زده می‌شود که به‌ازای پیش‌پردازش بلوک‌های اصلی BKZ 2.0 بوسیله‌یBKZ شامل تابع بازشماری، در بازه‌ی $۲^{۱۲} \leq \rho_۰ \leq ۲^{۱۵.۵}$ تخمین زده می‌شود و به‌ازای پیش‌پردازش بلوک‌ها اصلی BKZ 2.0 بوسیله‌ی BKZ شامل تابع غربال، این حد پایین تسریع زمانی در بازه‌ی $۰ \leq \rho_۰ \leq ۲^{۲۰.۵}$ تخمین زده می‌گردد. در نهایت، برای تعداد دور محدود N، تسریع زمانی حاصل از نسخه‌ی بازبینی شده‌ی ما از BKZ 2.0 نسبت به نسخه‌ی اصلی BKZ 2.0 برابر $O(min(\mathcal{N}, \rho_۰))$ تخمین می‌شود.

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

ISSN: 2322-4460