www.firstlight.cn
北京雷速科技有限公司

返回首页

# Ball-collision decoding

http://www.firstlight.cn　2010-11-19

This paper introduces a new generic decoding algorithm that is asymptotically faster than any previous attack against the McEliece cryptosystem. At a 256-bit security level, the attack costs 2.6 times fewer bit operations than the best previous attack; at a theoretical 1000-bit security level, the attack costs 15.5 times fewer bit operations than the best previous attack. The algorithm is asymptotically even faster than the Finiasz-Sendrier "lower bound" published at Asiacrypt 2009, demonstrating that the Finiasz-Sendrier parameter recommendations are not as secure as claimed. This paper proposes much safer, but still reasonably efficient, parameters based on an analysis of the fundamental bottleneck in all algorithms of this type.

存档文本