# Cryptology ePrint Archive: Report 2011/198

**Terminating BKZ**

*Guillaume Hanrot and Xavier Pujol and Damien Stehlé*

**Abstract:** Strong lattice reduction is the key element for most attacks against lattice-based cryptosystems. Between the strongest but impractical HKZ reduction and the weak but fast LLL reduction, there have been several attempts to find efficient trade-offs. Among them, the BKZ algorithm introduced by Schnorr and Euchner [FCT'91] seems to achieve the best time/quality compromise in practice. However, no reasonable complexity upper bound is known for BKZ, and Gama and Nguyen [Eurocrypt'08] observed experimentally that its practical runtime seems to grow exponentially with the lattice dimension. In this work, we show that BKZ can be terminated long before its completion, while still providing bases of excellent quality. More precisely, we show that if given as inputs a basis $(b_i)_{i\leq n} \in Q^{n \times n}$ of a lattice L and a block-size $\beta$, and if terminated after $\Omega\left(\frac{n^3}{\beta^2}(\log n + \log \log \max_i \|\vec{b}_i\|)\right)$ calls to a $\beta$-dimensional HKZ-reduction (or SVP) subroutine, then BKZ returns a basis whose first vector has norm $\leq 2 \gamma_{\beta}^{\frac{n-1}{2(\beta-1)}+\frac{3}{2}} \cdot (\det L)^{\frac{1}{n}}$, where~$\gamma_{\beta} \leq \beta$ is the maximum of Hermite's constants in dimensions $\leq \beta$. To obtain this result, we develop a completely new elementary technique based on discrete-time affine dynamical systems, which could lead to the design of improved lattice reduction algorithms.

**Category / Keywords:** public-key cryptography / Euclidean lattices, BKZ, lattice-based cryptanalysis

**Date:** received 18 Apr 2011

**Contact author:** xavier pujol at ens-lyon fr