Using the LLL-algorithm to Break the RSA Cryptosystem

Khoa Bui

Concordia University of Edmonton
Department of Mathematical and Physical Sciences

Abstract

The Rivest-Shamir-Adleman (RSA) cryptosystem is one of the most popular cryptosystems being used in secure data transmission. Until today, the cryptosystem is still considered to be safe due to the hardness of the factorization problem. The Lenstra-Lenstra-Lovász (LLL) algorithm offers various methods to attack the RSA cryptosystem, even going as far as potentially breaking the system by solving the factorization problem. In this presentation, we will discuss how a weak parameter creates deadly vulnerabilities in the RSA cryptosystem, and the usage of LLL-algorithm in the factorization problem.

Fig. 1: Source: Hartnett K.

https://www.quantamagazine.org/mathematicians-seal-back-door-to-breaking-rsa-encryption-20181217/

Definitions

1. Lattice: Let $n \geq 1$ and let $\vec{x}_1, \vec{x}_2, ..., \vec{x}_n$ be a basis in the euclidean space $\mathbb{R}^n$. The lattice with dimension n and basis $\vec{x}_1, \vec{x}_2, ..., \vec{x}_n$ is the set L of all linear combinations of the basis vectors with integrals coefficients [2].

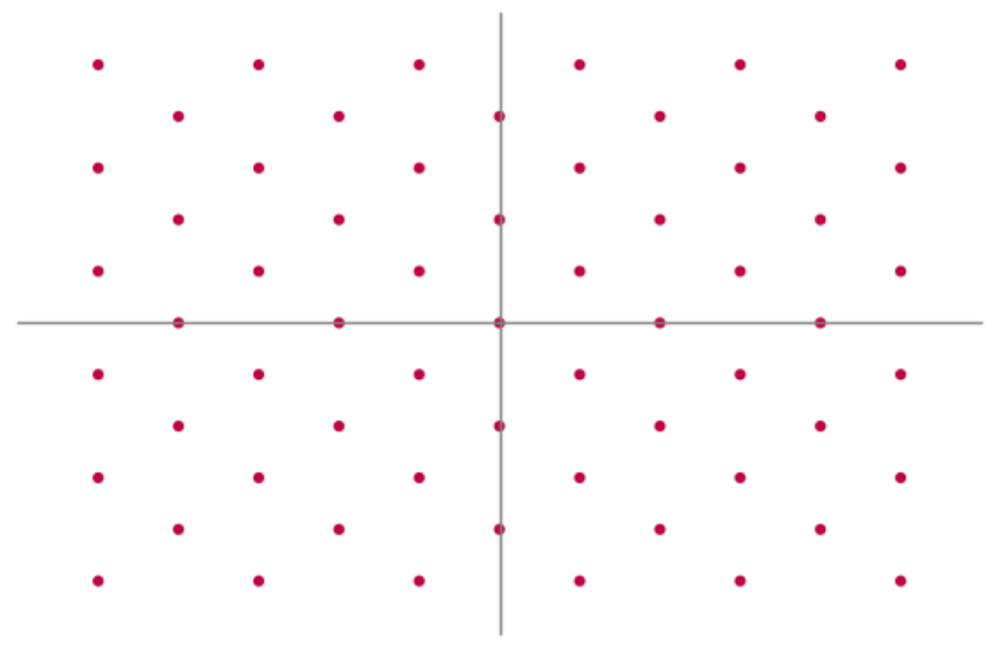

Fig. 2: Graphical representation of a lattice

2. The Lenstra–Lenstra–Lovász(LLL)-algorithm [2]:
   - *Input*: A basis $\vec{x}_1, \vec{x}_2, ..., \vec{x}_n$ of the lattice $L \subset \mathbb{R}^n$, and a reduction parameter $\alpha \in \mathbb{R}$ in the range $\frac{1}{4} < \alpha < 1$.
   - *Output*: A new basis with short vectors of lattice L.

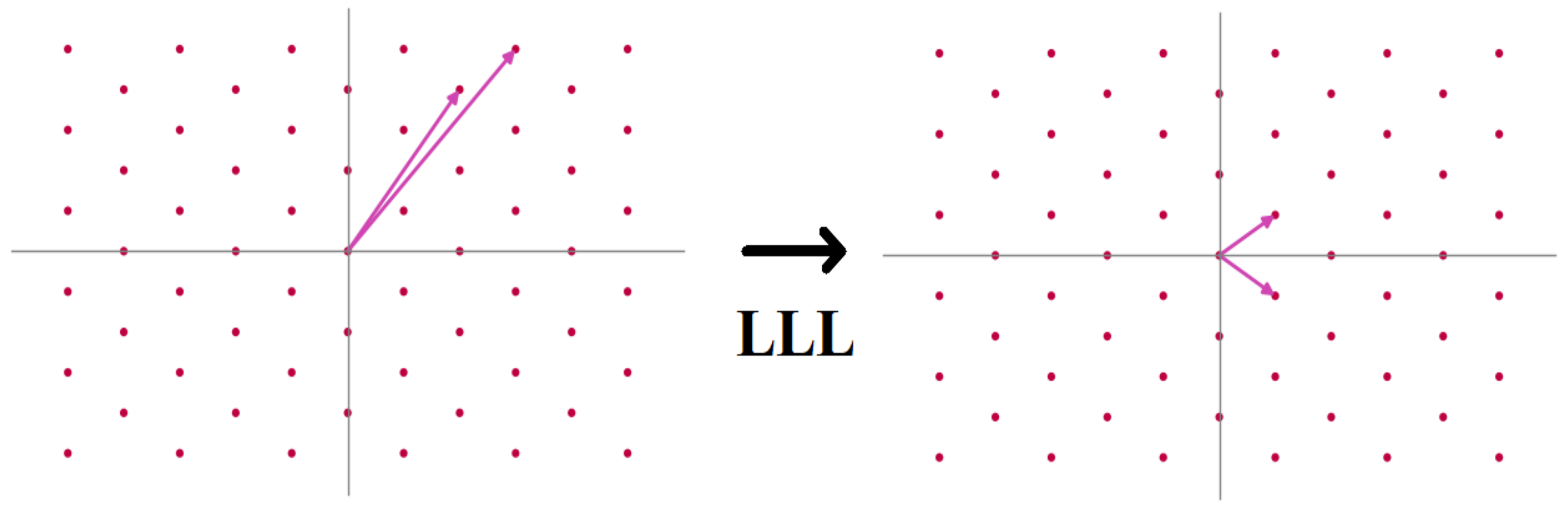

Fig. 3: Graphical representation of the LLL algorithm.

How does RSA work?

The RSA cryptosystem is an asymmetric cryptosystem, which means that it requires 2 keys, a public key and a private key, for the system to work. The public key is widely distributed for the purpose of encrypting information, while the private key is kept secret for the sake of security and decryption.

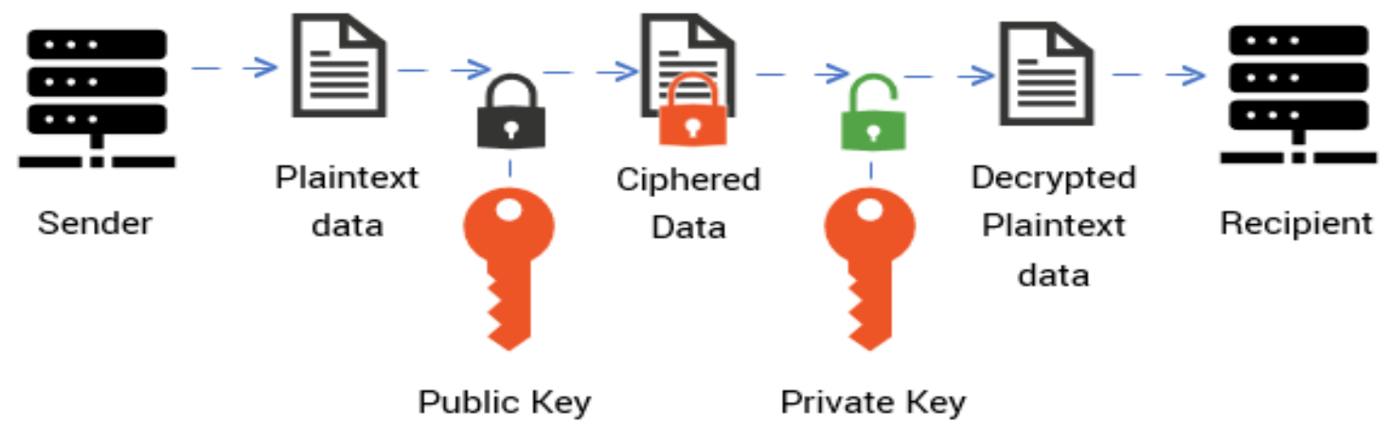

Fig. 4: Asymmetric cryptography.

Source: https://cheapsslsecurity.com/p/what-is-public-key-and-private-key-cryptography-and-how-does-it-work/

It is computationally very difficult to factor a large integer into its prime components; conversely, it is easy to find the product of two large prime numbers [3]. The RSA cryptosystem utilizes this fact to guarantee safe data transmission.

Using the LLL-algorithm to attack RSA

The Coppersmith's method is a LLL-algorithm based attack on low-public exponent RSA cryptosystems [1]. We have the following steps to the Coppersmith's method:

1. Translate RSA's encryption process $\boldsymbol{m} = \boldsymbol{c}^{\boldsymbol{e}} \mod \boldsymbol{N}$ into a monic polynomial equation.
2. Construct a Coppersmith's matrix.
3. Apply the LLL algorithm to the Coppersmith's matrix reducing it down to a polynomial.
4. Solve for the small roots of the polynomial.

Consequently [1], the root is the unknown part of the of the plaintext $\boldsymbol{m}$.

The LLL-algorithm in Coppersmith's method

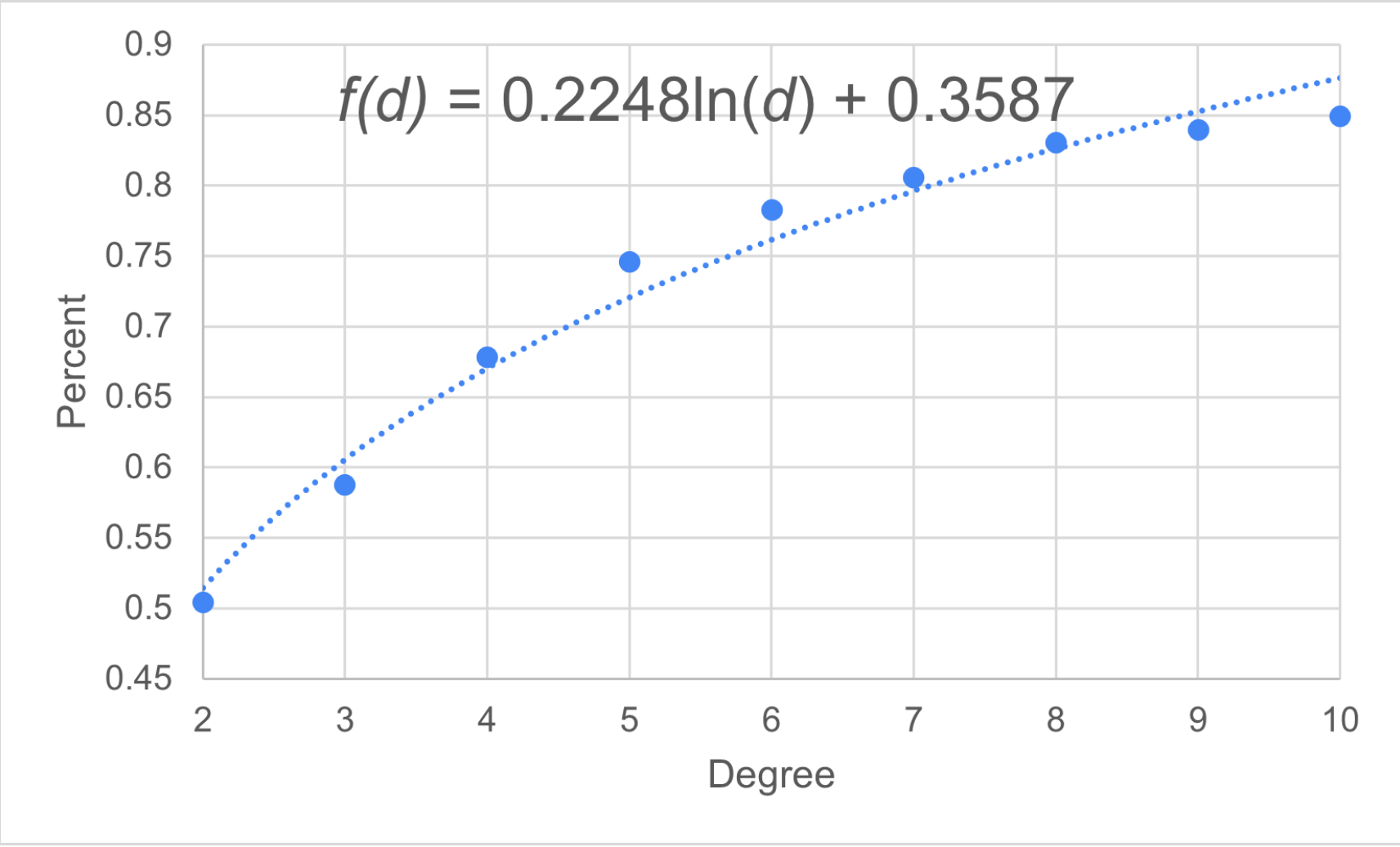

Fig. 5: Growth in percentage of lattice reduction steps

Experimental result suggests that the running time from the LLL algorithm steps quickly dominates the Coppersmith's method growing from half of the time to more than 90% of the Coppersmith's method.

Running time as a function of integer h and degree d

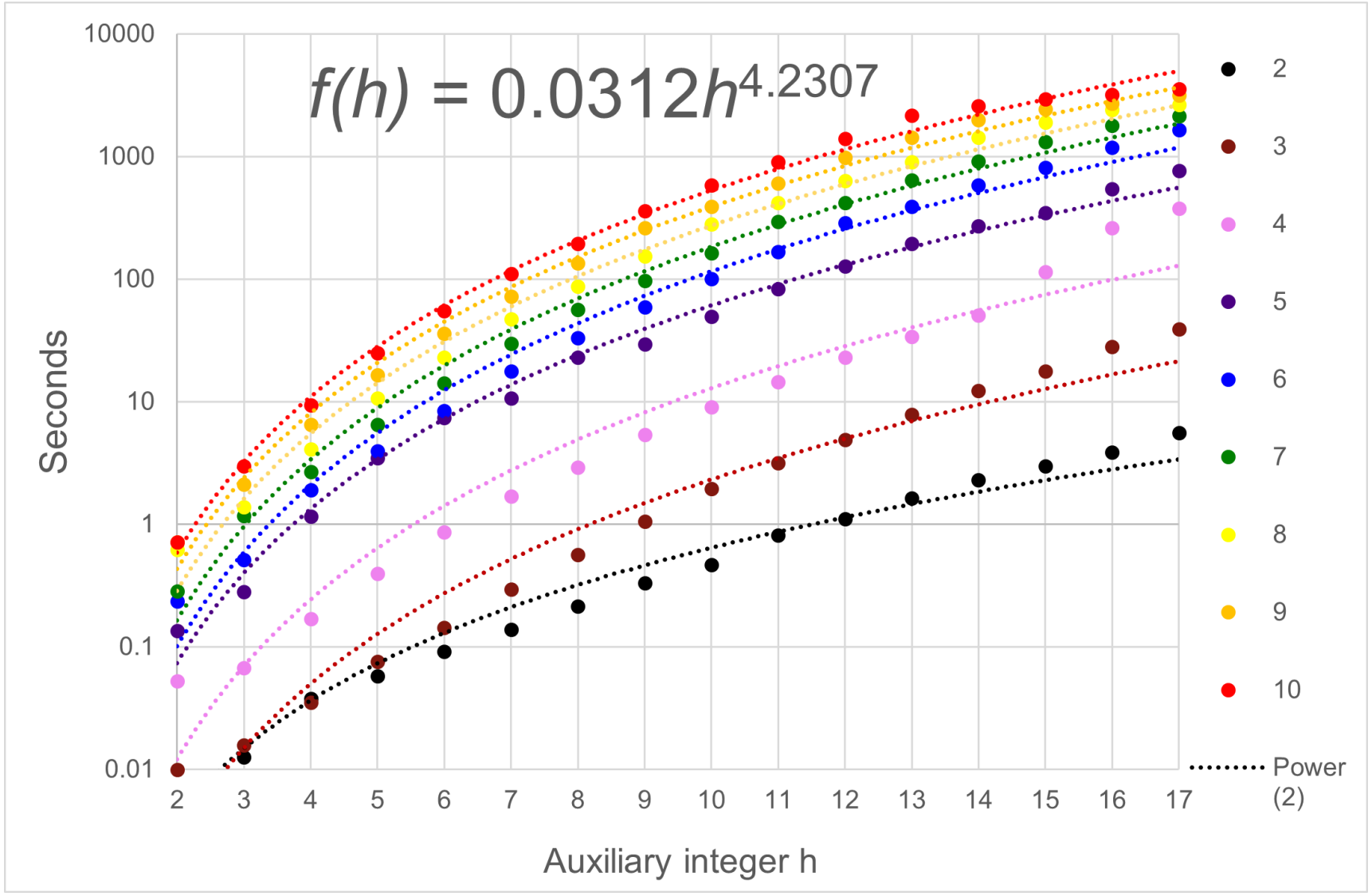

Fig. 6: Change in running time as a function of integer h

In Figure 6 the colours indicate the degree d corresponding with the integer h.

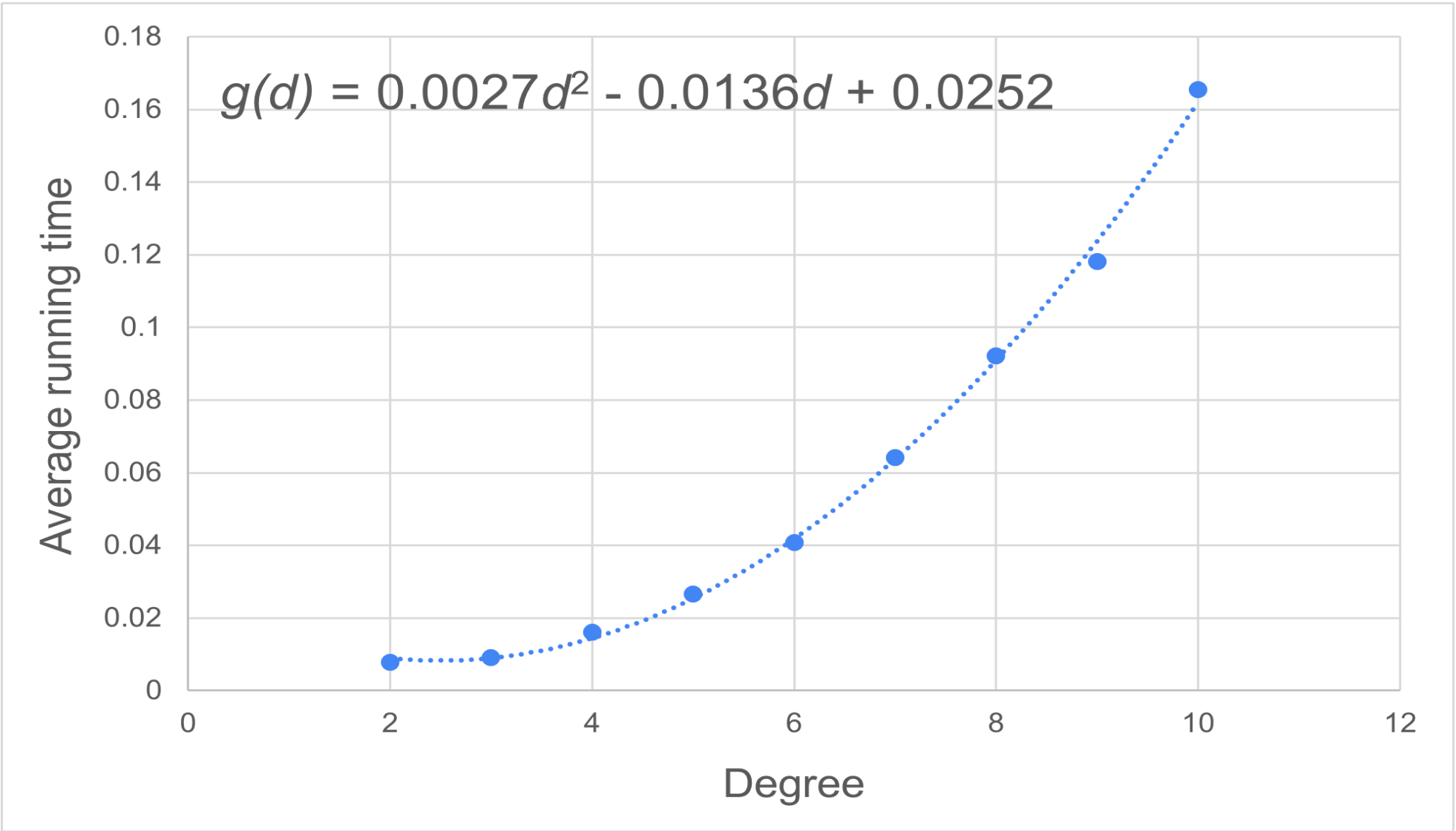

Fig. 7: Change in running time as a function of degree d

Conclusion and future work

Coppersmith's method offers an interesting use of the LLL-algorithm in attacking low exponent RSA cryptosystem. While the RSA cryptosystem is still secure for now, advancement in quantum computing might threaten the security of the system. On the LLL-algorithm, we can expect to see more applications of it in cryptography research in the near future.

Acknowledgement

My acknowledgement goes out to Dr. Tran, Dr. Huntemann, Dr. Guelzow, as well as my peers for advising and supervising this project.

References

[1] Don Coppersmith. "Small solutions to polynomial equations, and low exponent RSA vulnerabilities". In: *Journal of Cryptology* 10.4 (1997), pp. 233–260.

[2] Arjen K Lenstra, Hendrik Willem Lenstra, and László Lovász. "Factoring polynomials with rational coefficients". In: *Mathematische Annalen* 261.ARTICLE (1982), pp. 515–534.

[3] Ronald L Rivest, Adi Shamir, and Leonard Adleman. "A method for obtaining digital signatures and public-key cryptosystems". In: *Communications of the ACM* 21.2 (1978), pp. 120–126.