On the Hardness of LWE with Binary Error:

Revisiting the Hybrid Lattice-Reduction and Meet-in-the-Middle Attack

Johannes Buchmann[1] *and Florian Göpfert*[1] *and Rachel Player*[2] *and Thomas Wunderer*[1]

[1]Technische Universität Darmstadt, Germany

[2]Information Security Group, Royal Holloway, University of London, UK

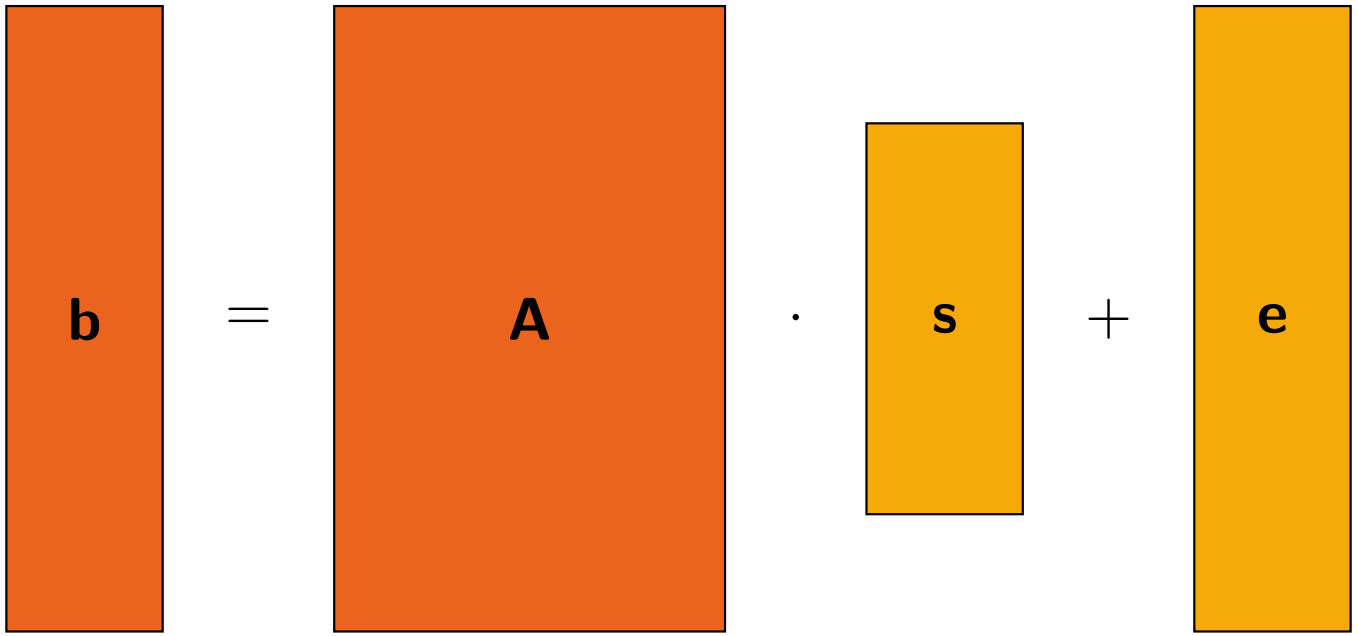
February 29, 2016

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Overview

Table of Contents

Learning with Errors (LWE)



- Given **A** and **b**, aim is to recover **s**
- Standard LWE: errors e_i are discrete Gaussian
- LWE with binary error: errors e_i are either 0 or 1
- Parameters: n (dimension), q (modulus).

Context

- LWE is a hardness assumption on which many cryptosystems are based
- (Standard) LWE is provably as hard as worst case lattice problems
- Picking parameters for schemes based on LWE (or variants thereof) is challenging
  - There are many possible attacks to consider
  - More attacks may apply to certain variants

Prior and related work

- 'Weak' LWE instances
- LWE with binary error
- Hybrid attack on NTRU

Prior and related work

'Weak' LWE instances

- Security of many schemes has been based on variants of LWE, such as:
  - Ring LWE
  - LWE with small secret
- This is for many reasons e.g. efficiency
- One can construct weak variants (e.g. [EHL14]), so caution must be taken

- LWE with binary error
- Hybrid attack on NTRU

Prior and related work

- 'Weak' LWE instances

LWE with binary error

- Introduced in [MP13]
  - Provided hardness result for $m = n + \mathcal{O}(n/\log n)$
- Considered in [ACF+14]
  - Provided subexponential attack when $m = \mathcal{O}(n \log\log n)$

- Hybrid attack on NTRU

Prior and related work

- 'Weak' LWE instances
- LWE with binary error

Hybrid attack on NTRU

- Introduced and analysed by Howgrave-Graham [How07]
- Hybrid attack:
  - Guess part of the secret: sped up by Meet-in-the-Middle
  - Lattice attack on a sublattice
- Additional analysis by Hirschhorn *et al.* [HHHW09]
- Mentioned in LWE context in [BG14]

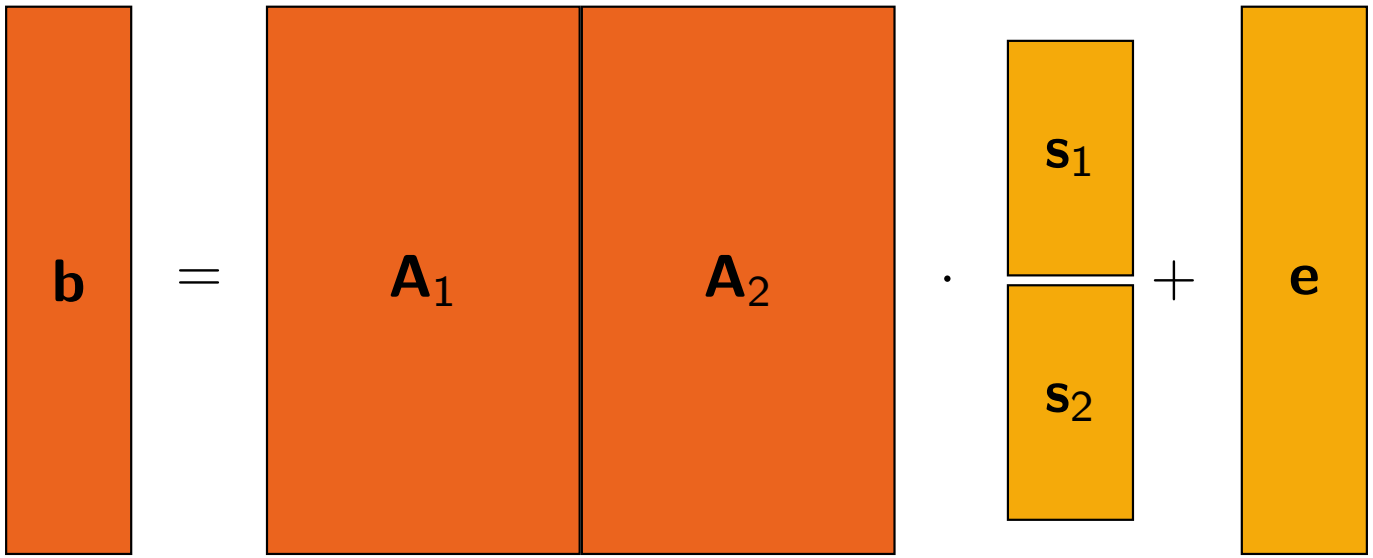
Table of Contents

Contributions

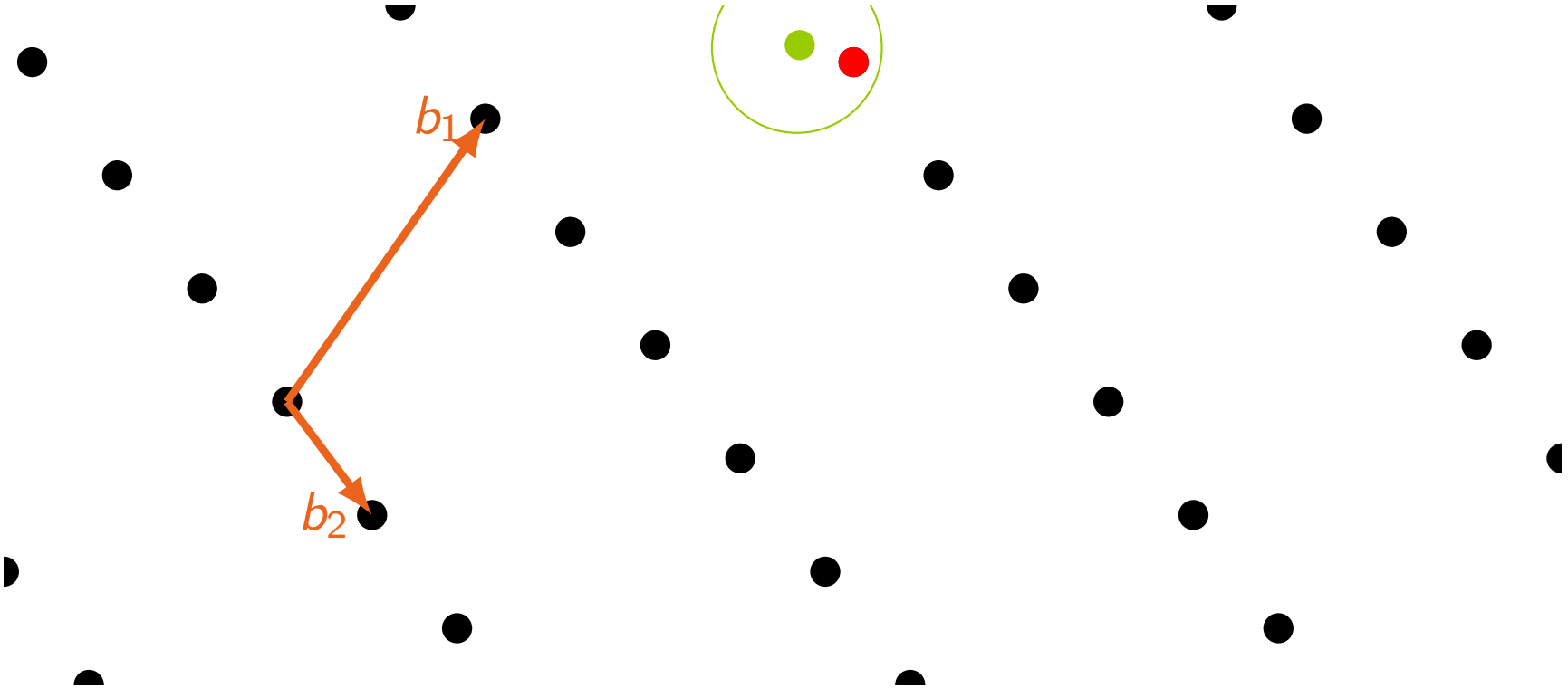
- Apply the hybrid attack to LWE with binary error
- Consider existing (general) LWE attacks applied to LWE with binary error
  - Show the hybrid attack outperforms other approaches for several natural choices of parameters
- Provide new analysis of the complexity of the hybrid attack
  - without experimental support required in [How07]
  - without additional assumption required in [HHHW09]

Algorithm (sketch)

- Guess vector $\mathbf{v}$ for first part of secret
- For correct guess $\mathbf{v} = \mathbf{s}_1$ it holds that $\mathbf{b} - \mathbf{A}_1\mathbf{v} = \mathbf{A}_2\mathbf{s}_2 + \mathbf{e}$
- Solve Bounded Distance Decoding on the $\mathbf{A}_2$ sublattice to recover $\mathbf{e}$
- Can speed up guess with Meet-in-the-Middle approach

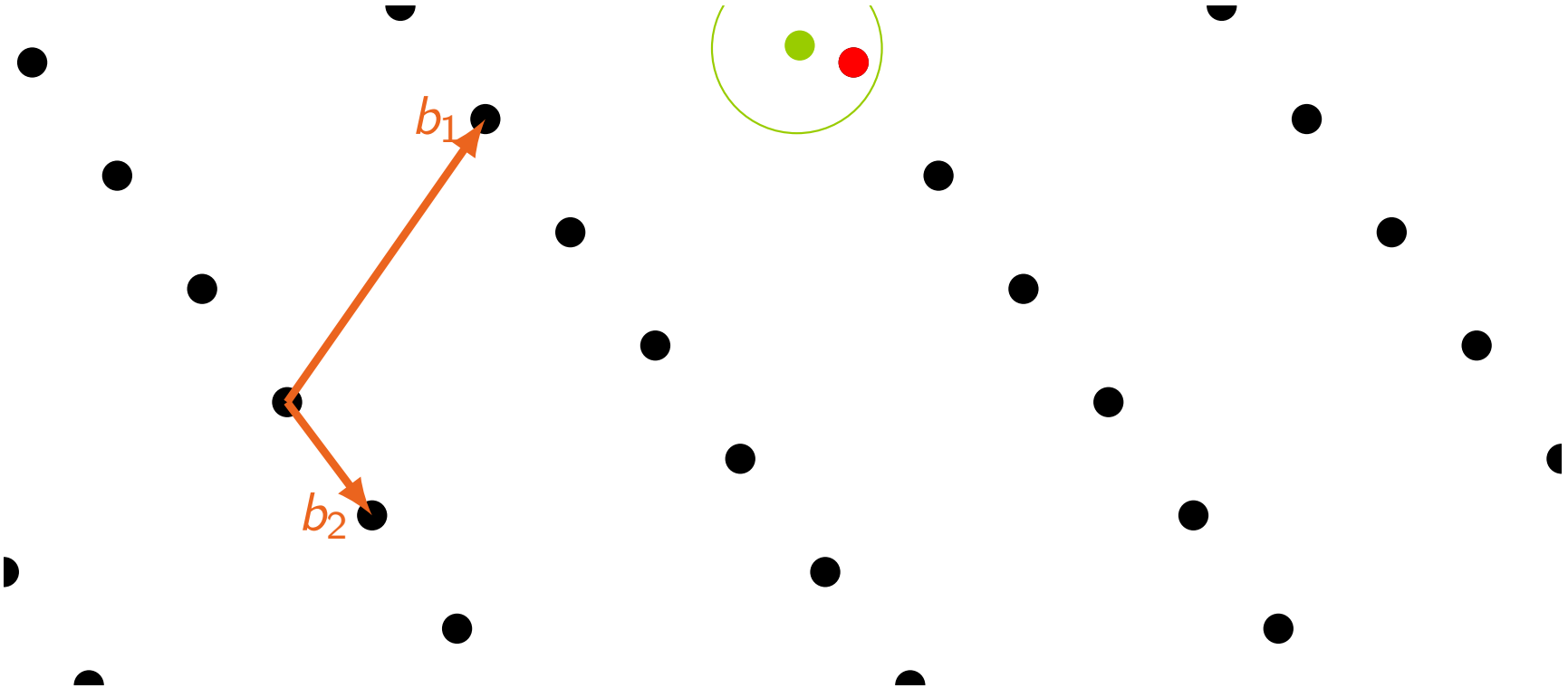


Bounded Distance Decoding (BDD)



Recover the closest lattice vector, given a target vector $\mathbf{t}$ and a basis $\mathbf{B}$ of the lattice.

Seeing LWE as a BDD problem



Recover the lattice point $\mathbf{A}_2\mathbf{s}_2$, given perturbed point $\mathbf{A}_2\mathbf{s}_2 + \mathbf{e}$ and basis $\mathbf{A}_2$ of the lattice.

Comparison (1)

- Many algorithms exist for solving LWE
- Most attacks can be adapted to LWE with binary error
  - Some, e.g. BKW require too many samples m
- We consider only the more efficient attacks; ruling out:
  - Meet-in-the-middle
  - Variants of Arora-Ge e.g. [ACF+14]

Comparison (2)

This leaves:

- Decoding attack
- uSVP attack
- Distinguishing attack

We describe how the existing estimates of complexity of these attacks can be altered in the LWE with binary error case.

Comparison (3)

n	q	$\log_2(T_{\text{Hybrid attack}})$	$\log_2(T_{\text{Decoding}})$	$\log_2(T_{\text{uSVP}})$	$\log_2(T_{\text{Distinguishing}})$
128	256	**41**	67	82	**37**
160	256	**55**	77	122	**62**
192	256	**71**	88	162	**85**
224	256	**87**	**102**	165	109
256	256	**103**	**117**	203	132
288	256	**120**	**136**	254	154
320	256	**136**	**158**	327	176
352	256	**153**	**185**	443	198

Comparison of attacks on LWE with binary error using at most $m = 2n$ samples. $\log_2 T_{\text{attack}}$ denotes the bit operations required to solve using the approach 'attack'.

Table of Contents

Conclusion

- While variants of LWE can be attractive, care must be taken
  - More attacks may apply than in the standard LWE case
- In particular, hybrid attack is effective against LWE with binary error
  - Should be taken into account when choosing parameters in this case

Thank you!

Paper available at:
`https://eprint.iacr.org/2016/089`

Questions?

Selected Bibliography

[ACF+14] Martin R. Albrecht, Carlos Cid, Jean-Charles Faugère, Robert Fitzpatrick, and Ludovic Perret. Algebraic algorithms for LWE problems. *IACR Cryptology ePrint Archive*, 2014:1018, 2014.

[BG14] Shi Bai and Steven D. Galbraith. Lattice decoding attacks on binary LWE. In Willy Susilo and Yi Mu, editors, *ACISP 2014, Wollongong, NSW, Australia, July 7-9, 2014. Proceedings*, volume 8544 of *Lecture Notes in Computer Science*, pages 322–337. Springer, 2014.

[EHL14] Kirsten Eisenträger, Sean Hallgren, and Kristin E. Lauter. Weak instances of PLWE. In Antoine Joux and Amr M. Youssef, editors, *SAC 2014, Montreal, QC, Canada, August 14-15, 2014, Revised Selected Papers*, volume 8781 of *Lecture Notes in Computer Science*, pages 183–194. Springer, 2014.

[HHHW09] Philip S. Hirschhorn, Jeffrey Hoffstein, Nick Howgrave-Graham, and William Whyte. Choosing NTRUEncrypt parameters in light of combined lattice reduction and MITM approaches. In Michel Abdalla, David Pointcheval, Pierre-Alain Fouque, and Damien Vergnaud, editors, *ACNS 2009*, volume 5536 of *Lecture Notes in Computer Science*, pages 437–455, 2009.

Selected Bibliography (cont.)

[How07] Nick Howgrave-Graham. A hybrid lattice-reduction and meet-in-the-middle attack against NTRU. In Alfred Menezes, editor, *CRYPTO 2007, Santa Barbara, CA, USA, August 19-23, 2007, Proceedings*, volume 4622 of *Lecture Notes in Computer Science*, pages 150–169. Springer, 2007.

[MP13] Daniele Micciancio and Chris Peikert. Hardness of SIS and LWE with small parameters. In Ran Canetti and Juan A. Garay, editors, *CRYPTO 2013, Santa Barbara, CA, USA, August 18-22, 2013. Proceedings, Part I*, volume 8042 of *Lecture Notes in Computer Science*, pages 21–39. Springer, 2013.