RSAConference2021

May 17 – 20 | Virtual Experience

RESILIENCE

SESSION ID: **CRYP-W13C**

On the Hardness of Module-LWE with Binary Secrets

Corentin Jeudy

Research Intern
Univ Rennes, CNRS, IRISA
Co-authors: Katharina Boudgoust, Adeline Roux-Langlois, Weiqiang Wen

Our Result (https://ia.cr/2021/265)

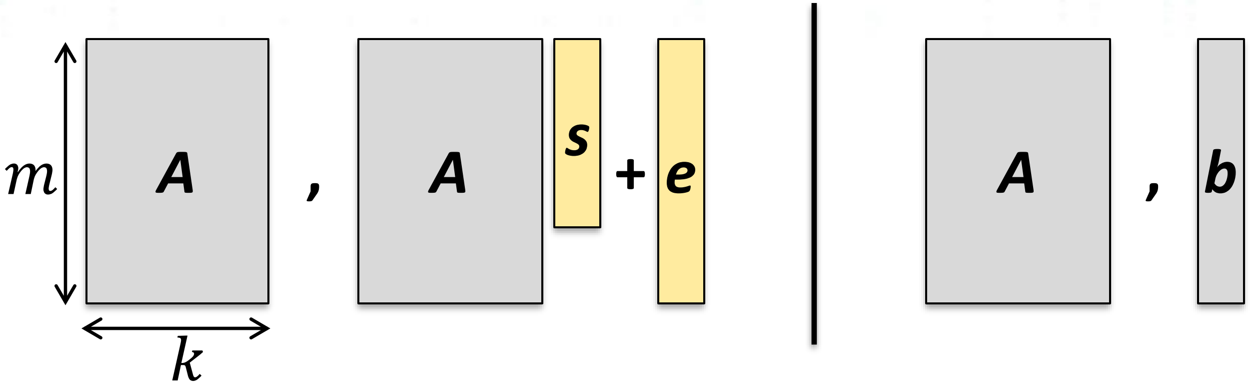
We (im)prove the theoretical hardness of **Module Learning With Errors** with **Binary Secrets**

- Over **cyclotomic fields** (degree n)
- For a **super-logarithmic module rank**: $d = \omega(\log n)$
- Down to **linearly small modulus**: $q \geq 2n$
- With a **small noise increase**: $\beta = \alpha \cdot \Theta(n^2\sqrt{d})$

We reduce the gap between **theoretical** and **practical** hardness when using small secrets

Module Learning With Errors (M-LWE)

The M-LWE problem asks to distinguish between two cases:



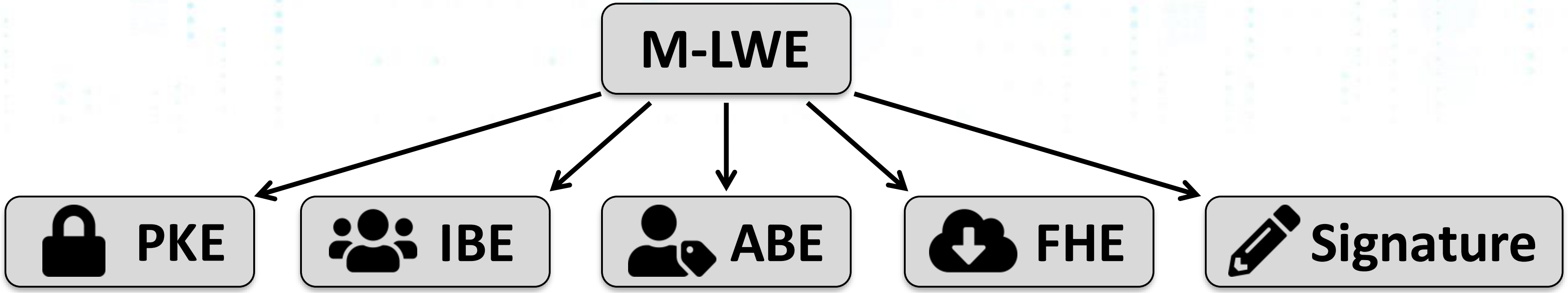
where $\boldsymbol{A} \hookleftarrow U(R_q^{k\times m})$, $\boldsymbol{s} \hookleftarrow U(R_q^k)$, $\boldsymbol{e} \hookleftarrow D_{R,\alpha q}^m$, and $\boldsymbol{b} \hookleftarrow U\left(R_q^m\right)$

$R = \mathbb{Z}[x]/\langle\Phi(x)\rangle$ is a cyclotomic ring with $\deg(\Phi) = n$. A popular choice is $n = 2^\ell$ yielding $\Phi(x) = x^n + 1$. We work in $R_q = \mathbb{Z}_q[x]/\langle\Phi(x)\rangle$.

Binary Secrets: $\boldsymbol{s}$ chosen from $R_2^k = (\mathbb{Z}_2[x]/\langle\Phi(x)\rangle)^k$

Edge cases: LWE ($n = 1 \Rightarrow R = \mathbb{Z}$) and R-LWE ($k = 1$)

Apply Module-LWE, Why Do We Care?



Key Encapsulation Mechanisms

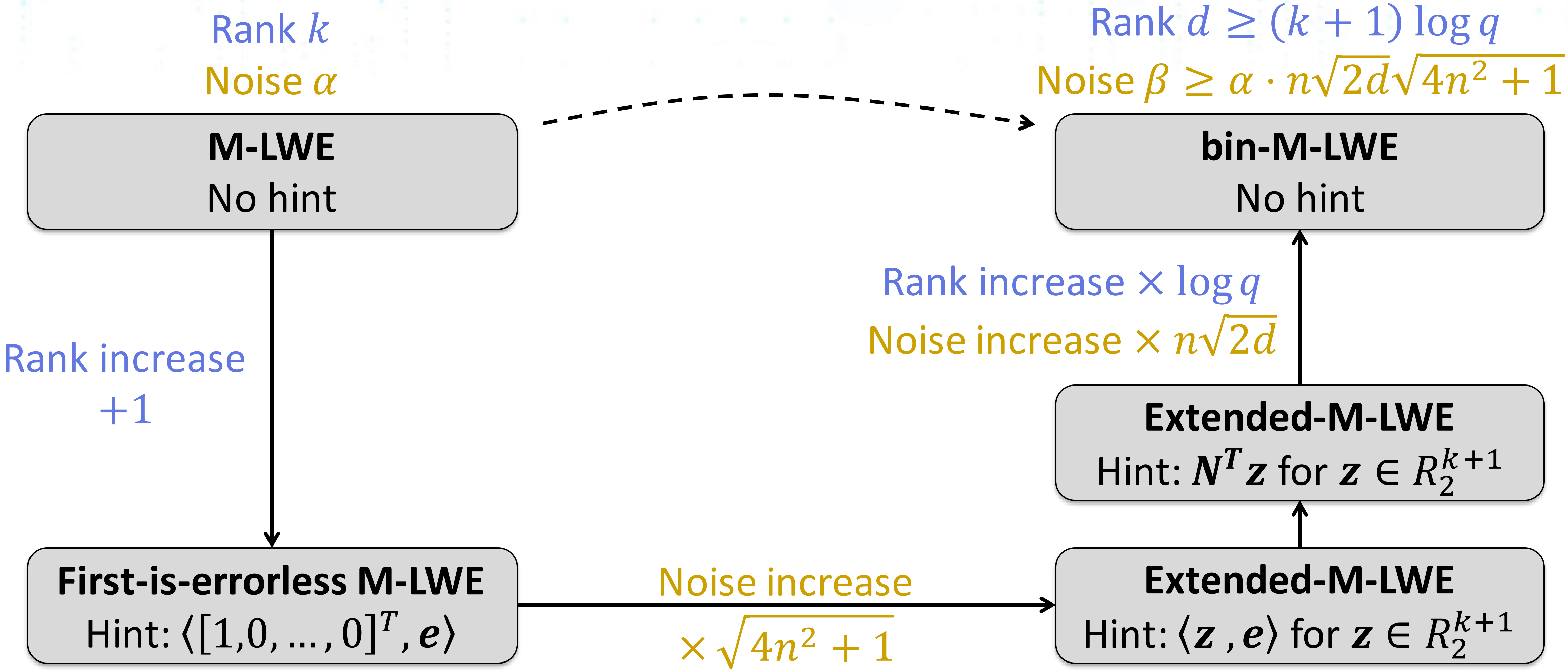
- **CRYSTALS-KYBER** [BDK+18]: based on Module-LWE
- **SABER** [DKRV18]: based on Module-LWR (deterministic)

Signature Schemes

- **CRYSTALS-DILITHIUM** [DKL+18]: based on Module-LWE

"*In NIST's current view, these structured lattice schemes appear to be the most promising general-purpose algorithms for public-key encryption/KEM and digital signature schemes*.", Third Round Candidate Announcement, July 22, 2020

Proof Structure following [BLP+13]



First-is-errorless M-LWE to Extended M-LWE: Construction

Reduction from first-is-errorless M-LWE to ext-M-LWE requires to construct, for any given $\boldsymbol{z} \in R_2^d$, a matrix $\boldsymbol{U}_{\boldsymbol{z}}$ such that

- $\boldsymbol{U}_{\boldsymbol{z}}$ is invertible in R_q
- $(\boldsymbol{U}_{\boldsymbol{z}}^{\perp})^T \boldsymbol{z} = \boldsymbol{0}$
- with minimal spectral norm (characterizes the noise growth)

$$\boldsymbol{z} = [z_1, \ldots, z_d]^T \in R_2^d$$

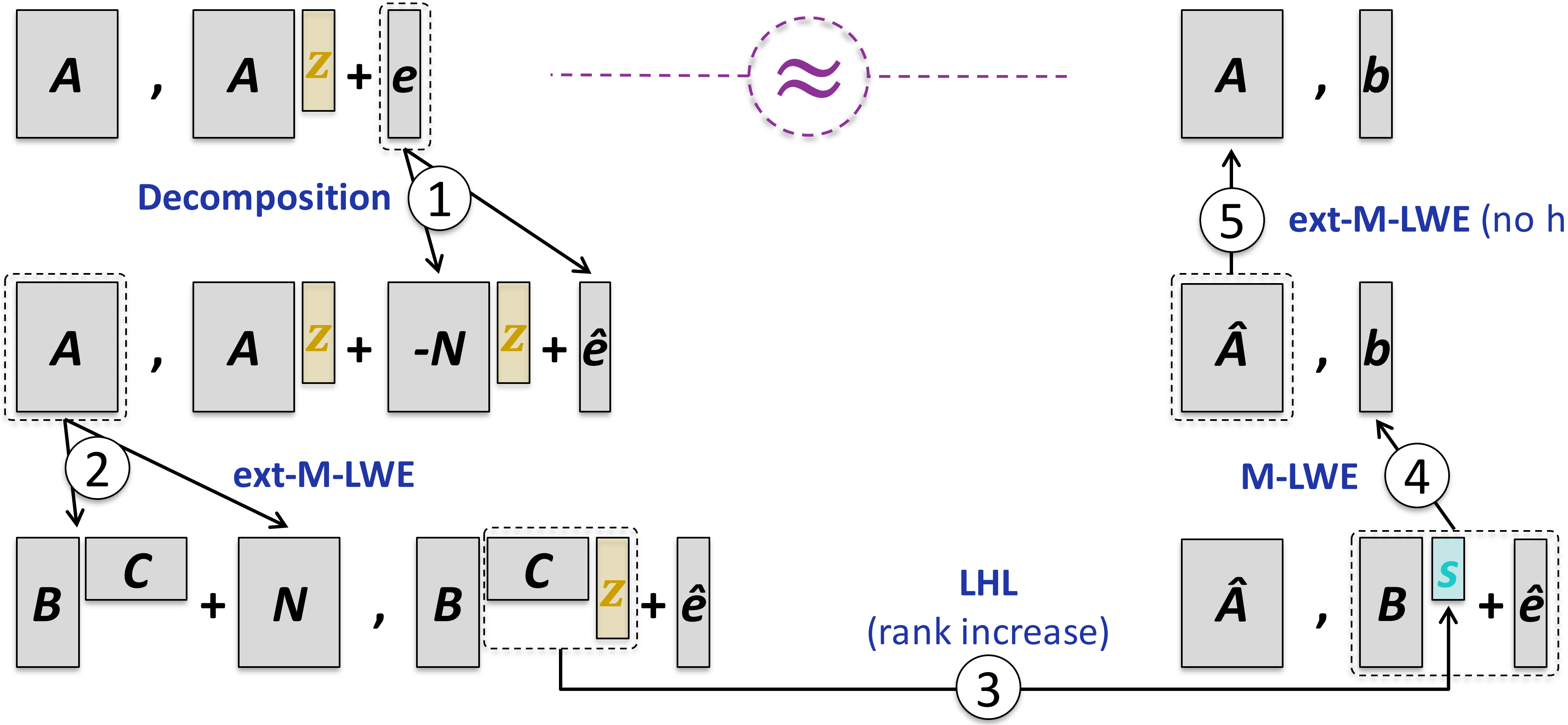
$$\boldsymbol{U}_{\boldsymbol{z}} = \begin{bmatrix} 1 & -z_2 & & \\ & z_1 & \ddots & \\ & & \ddots & -z_d \\ & & & z_{d-1} \end{bmatrix} \in R^{d \times d}$$

$\boldsymbol{U}_{\boldsymbol{z}}^{\perp}$

- ✔ Invertibility: restriction on q [LS18]
- ✔ Orthogonality: trivial
- ✔ Spectral norm: $\leq 2n$

Reduction to bin-M-LWE: Lossy Argument

Lossy argument: replacing $\boldsymbol{A}$ by $\hat{\boldsymbol{A}} = \boldsymbol{BC} + \boldsymbol{N}$. The secret $\boldsymbol{z}$ is binary and the secret $\boldsymbol{s}$ is modulo q.



Conclusion

Related Work

- Setting $n = 1$ yields the result from [BLP+13]
- Our previous reduction [BJRW20] achieves similar rank d and modulus q, but larger noise growth $\beta/\alpha = \Theta(n^2 d\sqrt{m})$. We improve it by a factor of $\sqrt{md}$

Open Problems

- Smaller ranks: rank $d = 1$ (R-LWE)
- Other number fields than cyclotomics

RSAConference2021

Thank You!

[BDK+18] J. W. Bos, L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, J. M. Schanck, P. Schwabe, G. Seiler, and D. Stehlé.
CRYSTALS – Kyber: A CCA-secure Module-Lattice-based KEM.
In *2018 IEEE European Symposium on Security and Privacy, EuroS&P 2018, London, United Kingdom, April 24-26, 2018,* pages 353-367, 2018.

[BJRW20] K. Boudgoust, C. Jeudy, A. Roux-Langlois, W. Wen.
Towards Classical Hardness of Module-LWE: The Linear Rank Case.
In *Advances in Cryptology – ASIACRYPT 2020 – 26th International Conference on the Theory and Application of Cryptology and Information Security, Daejeon, South Korea, December 7-11, 2020, Proceedings, Part II,* volume 12492 of *Lecture Notes in Computer Science,* pages 289-317. Springer, 2020

[BLP+13] Z. Brakerski, A. Langlois, C. Peikert, O. Regev, and D. Stehlé.
Classical Hardness of Learning With Errors.
In *Symposium on Theory of Computing Conference, STOC'13, Palo Alto, CA, USA, June 1-4, 2013,* pages 575-584, 2013.

[DKL+18] L. Ducas, E. Kiltz, T. Lepoint, V. Lyubashevsky, P. Schwabe, G. Seiler, and D. Stehlé.
CRYSTALS – Dilithium: A Lattice-based Digital Signature Scheme.
IACR Trans. Cryptogr. Hardw. Embed. Syst., 2018(1):238-268, 2018.

[DKRV18] J.-P. D'Anvers, A. Karmakar, S. Sinha Roy, and F. Vercauteren.
SABER: Module-LWR based Key Exchange, CPA-secure Encryption and CCA-secure KEM.
In *Progress in Cryptology – AFRICACRYPT 2018 – 10th International Conference on Cryptology in Africa, Marrakesh, Morocco, May 7-9, 2018, Proceedings,* pages 282-305, 2018.

[LS18] V. Lyubashevsky and G. Seiler
Short, Invertible Elements in Partially Splitting Cyclotomic Rings and Applications to Lattice-based Zero-Knowledge Proofs.
In *Advances in Cryptology – EUROCRYPT 2018 – 37th Annual International Conference on the Theory and Applications of Cryptographic Techniques, Tel Aviv, Israel, April 29 – May 3, 2018, Proceedings, Part I*, volume 10820 of *Lecture Notes in Computer Science*, pages 204-224. Springer, 2018.