

Lattice Assumption Zoo

Jan Niklas Siemer
King's College London
July 13, 2026





- Cryptographic Primitives and Hard Problems in Cryptography Wiki
 - Website hosted by Frederik Vercauteren in Leuven
 - Project was discontinued around 2012
- Is it broken yet?
- SIS with Hints Zoo
 - Name inspired by Complexity Zoo



- Cryptographic Primitives and Hard Problems in Cryptography Wiki
 - Website hosted by Frederik Vercauteren in Leuven
 - Project was discontinued around 2012
- Is it broken yet?
- SIS with Hints Zoo
 - Name inspired by Complexity Zoo

Shared Issue

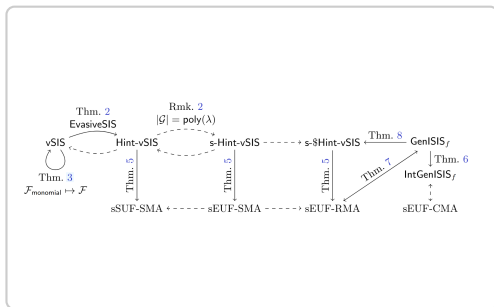
- Little to no structure to get a meaningful high-level overview
 - Complexity Zoo provides complexity classes by starting symbols and refers to external resources for first steps
 - “Is it broken yet?” and “SIS with Hints Zoo” provide tags: STANDARD, EQUIVALENT, BROKEN
- Becomes a problem once a field becomes complex



Solution: A Graph

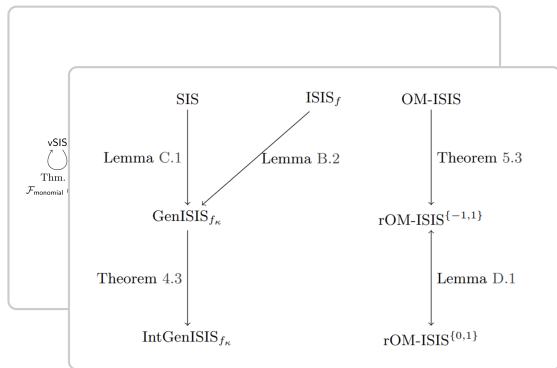


Solution: A Graph



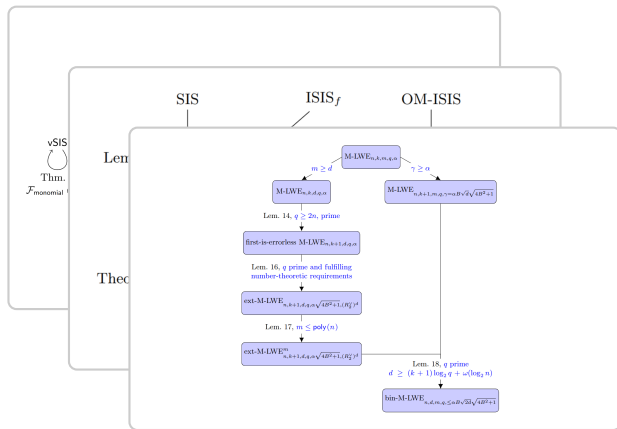


Solution: A Graph



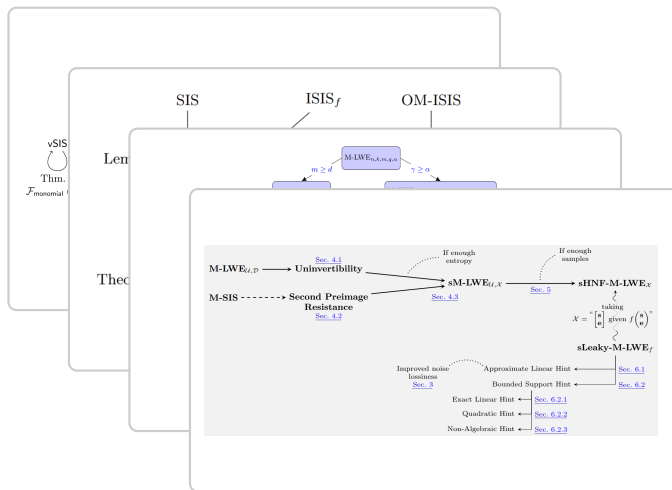


Solution: A Graph



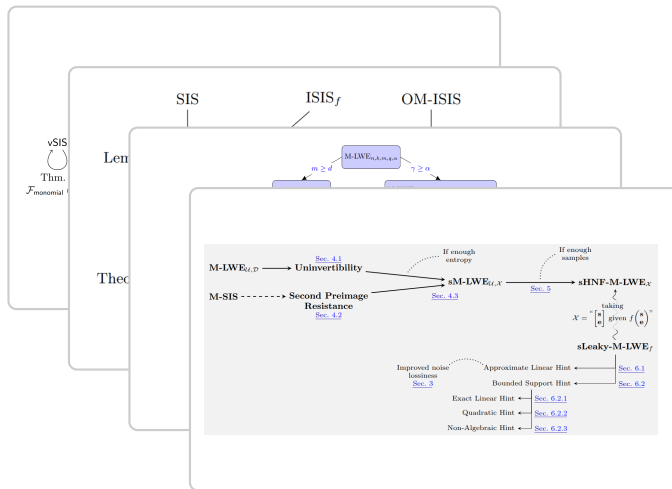


Solution: A Graph



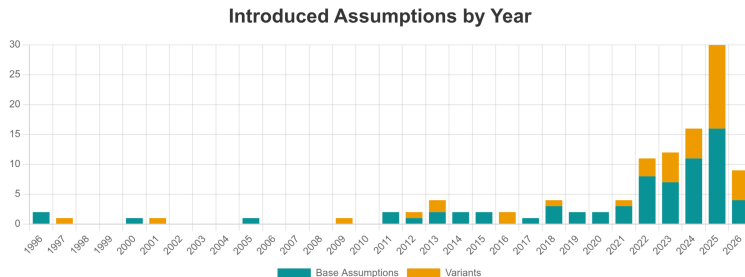


Solution: A Graph – trades granularity of information for simplicity of insights





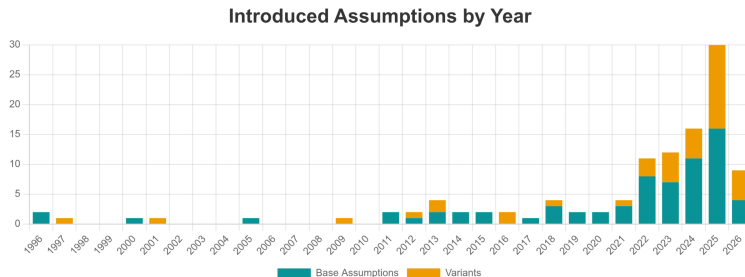
- Landscape of lattice-based assumptions evolves quickly



- Heterogeneous group of authors introducing new assumptions $\Rightarrow$ Requires a heterogeneous group to track them $\Rightarrow$ Format needs to encourage contributions
- Provides freedom in presentation of assumptions
 - Simplified descriptions of assumptions to convey intuition
 - Adapt notation to conventions in area of utilisation



- Landscape of lattice-based assumptions evolves quickly



- Heterogeneous group of authors introducing new assumptions $\Rightarrow$ Requires a heterogeneous group to track them $\Rightarrow$ Format needs to encourage contributions
 - Provides freedom in presentation of assumptions
 - Simplified descriptions of assumptions to convey intuition
 - Adapt notation to conventions in area of utilisation
- $\Rightarrow$ Public wiki with space for unstructured data s.t. anyone can contribute is most likely to be able to capture this development



- Wiki software (e.g. MediaWiki) is mostly built for unstructured data
- ⇒ Missing features to store structured information to populate e.g. a graph or tags

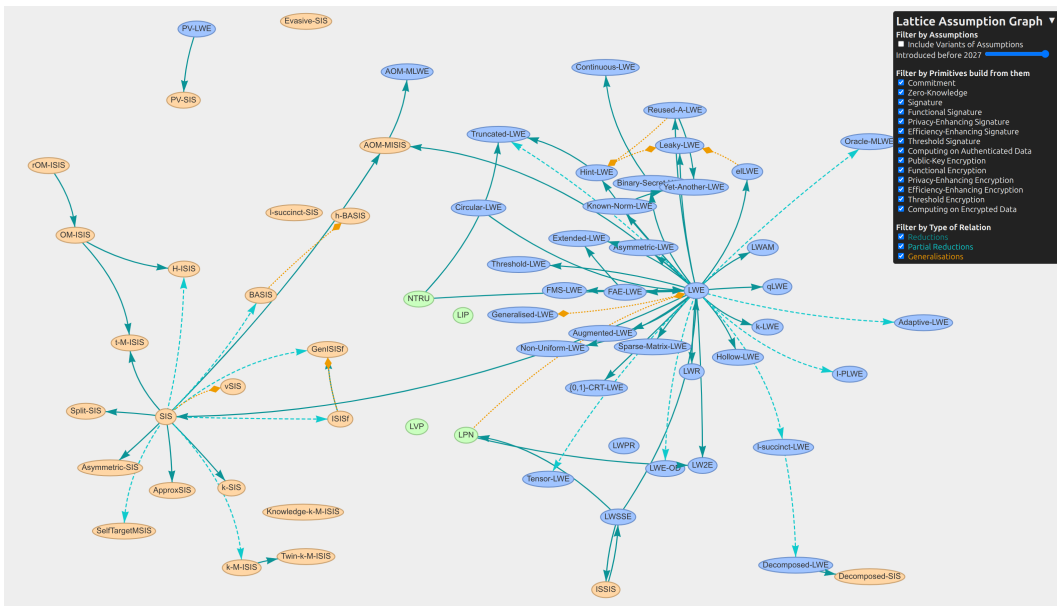


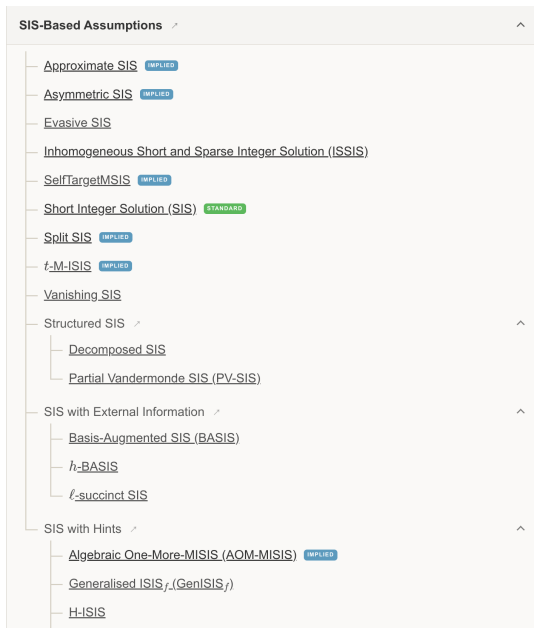
- Wiki software (e.g. MediaWiki) is mostly built for unstructured data
- ⇒ Missing features to store structured information to populate e.g. a graph or tags

Solution

- Website with space for structured and unstructured data utilising Markdown files (with some structured YAML data) to store both
- Use git workflow with Pull Requests to ensure structured data is synchronised with unstructured data
- Website uses static site generator called Jekyll (default for Github Pages) to generate website from Markdown files with LaTeX and Bibtex support
- If you want to contribute
 - Simple Markdown environment + typical git workflow
 - Extensive guidance available if needed
 - Hosting website locally to check changes easy via Docker

Structured Visualisations to Explore Landscape – Graph



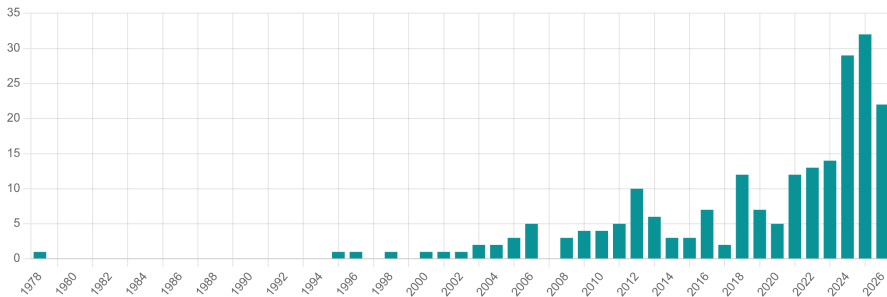


- Catalogue with families and subfamilies of assumptions
- Built-in search engine
- Random assumption button



- >70 assumptions (>110 if we count variants)
 - Too many assumptions: Yet-Another LWE, (Yet-Another)² LWE
- 6 Contributors
- Relies on information of more than 200 papers

Cited Publications by Year



Assumptions with Negative Cryptanalytic Evidence



Knowledge k -R-ISIS

Proposed by Martin R. Albrecht, Valerio Cini, Russell W. F. Lai, Giulio Malavolta, and Sri Aravinda Krishnan Thyagarajan in 2022.

Invalidated by Hoeteck Wee and David J. Wu, at least morally.



Partial-Vandermonde Knapsack Family

Proposed by Hoffstein, Pipher, Schanck, Silverman, and Whyte in 2014.

Attacked by Katharina Boudgoust, Erell Gachon, and Alice Pellet-Mary.

Evasive LWE

Proposed by Hoeteck Wee in 2022.

Counterexamples on several variants by

- Chris Brzuska, Akin Ünal, and Ivy K. Y. Woo
- Shweta Agrawal, Anuja Modi, Anshu Yadav, and Shota Yamada
- Nico Döttling, Abhishek Jain, Giulio Malavolta, Surya Mathialagan, and Vinod Vaikuntanathan



Binary-Matrix LWE

Proposed by Galbraith in 2013.

Optimistic parameters broken by Herold and May.

Adaptive LWE

Proposed by Quach, Wee, and Wichs in 2018.

Optimistic parameters broken by Abram, Malavolta, and Roy.

Oracle M-LWE

Proposed by Liu, Sotiraki, Tromer, and Wang in 2025.

Optimistic parameters broken by Wang, Esgin, Steinfeld, Saarinen, and Yiu.



Still “Under Construction” mainly due to two reasons

- Finishing up 4 more involved assumptions (Evasive LWE , MLWE-PRF-RU , MP-LWE , MP-LWR)
- Experience from prior conferences: list of missing assumptions will grow

Optimistic that we can remove the “Under Construction” banner in three weeks.



Still “Under Construction” mainly due to two reasons

- Finishing up 4 more involved assumptions (Evasive LWE, MLWE-PRF-RU, MP-LWE, MP-LWR)
- Experience from prior conferences: list of missing assumptions will grow

Optimistic that we can remove the “Under Construction” banner in three weeks.

But even if we can remove the banner, this doesn't imply that every page is perfect.

- Several pages *only* contain existence statements for reductions but lack description of intuition behind this reduction.
- ⇒ Hopefully you join in and provide intuitions and descriptions of assumptions, reductions, or cryptanalytic approaches wherever you're familiar with the topic.

Thanks for your Attention!



<https://latticeassumptionzoo.org>



[https://github.com/jnsiemer/
latticeassumptionzoo](https://github.com/jnsiemer/latticeassumptionzoo)