Salsa Verde versus the Actual State of the Art

Léo Ducas,
Eamonn Postlethwaite
Jana Sotáková

August 2023
(kindly represented by Thomas Espitau)

SALSA VERDE: a machine learning attack on Learning With Errors with sparse small secrets

Cathy Li **Jana Sotáková** **Emily Wenger** **Zeyuan Allen-Zhu**
Francois Charton* **Kristin Lauter***
Meta AI

Custom instances of LWE that seem to be tackled by ML
(very sparse secret, and sometimes large modulus q)

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time			uSVP attack time (hrs)
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total (hrs)*	
12	8	1.5	2 epochs	4.5	N/A
14	12	2.5	2-5 epochs	5.5-10	N/A
16	14	8.0	2 epochs	11	N/A
18	18	7.0	3 epochs	11.5	558
18	20	7.0	1-8 epochs	8.5-19	259
20	22	7.5	5 epochs	15	135-459
20	23	7.5	3-4 epochs	12-15	167-330
20	24	7.5	4 epochs	13.5	567
20	25	7.5	5 epochs	15	76 - 401

To summarize the comparison, VERDE outperforms existing classical attacks in two senses: 1) VERDE fully recovers sparse binary and ternary secrets for n and q where existing classical attacks do not succeed in several weeks or months using *fplll* BKZ 2.0 [19] with the required block size;

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time			State of the Art Attack (hrs)
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total (hrs)*	
12	8	1.5	2 epochs	4.5	**0.2 (MITM)**
14	12	2.5	2-5 epochs	5.5-10	Implementation in Progress
16	14	8.0	2 epochs	11	
18	18	7.0	3 epochs	11.5	
18	20	7.0	1-8 epochs	8.5-19	(Hybrid MITM-Lattice) Models and predictions, exists, but no open source implem.
20	22	7.5	5 epochs	15	
20	23	7.5	3-4 epochs	12-15	
20	24	7.5	4 epochs	13.5	
20	25	7.5	5 epochs	15	**12 -- 24 (rescaled uSVP)**

To summarize the comparison, VERDE outperforms existing classical attacks in two senses: 1) VERDE fully recovers sparse binary and ternary secrets for n and q where existing classical attacks do not succeed in several weeks or months using *fplll* BKZ 2.0 [19] with the required block size;

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time				State of the Art Attack (hrs, 1core)
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total*	(hrs × CPU)	
12	8	1.5	2 epochs	4.5	× ???	**0.2 (MITM … in Py)**
14	12	2.5	2-5 epochs	5.5-10	× 270	Implementation in Progress
16	14	8.0	2 epochs	11	× ???	
18	18	7.0	3 epochs	11.5	× 990	
18	20	7.0	1-8 epochs	8.5-19	× ???	(Hybrid MITM-Lattice) Models and predictions, exists, but no open source implem.
20	22	7.5	5 epochs	15	× ???	
20	23	7.5	3-4 epochs	12-15	× ???	
20	24	7.5	4 epochs	13.5	× ???	
20	25	7.5	5 epochs	15	× ???	**12 -- 24 (rescaled uSVP)**

To summarize the comparison, VERDE outperforms existing classical attacks in two senses: 1) VERDE fully recovers sparse binary and ternary secrets for n and q where existing classical attacks do not succeed in several weeks or months using *fplll* BKZ 2.0 [19] with the required block size;

Table 15. Comparison of VERDE's and uSVP attack performance on LWE problems with $n = 256$, binary secrets, varying q and h. *VERDE's total attack time is the sum of preprocessing and training time (with recovery included). Preprocessing time assumes full parallelization, and training time is the number of epochs to recovery multiplied by epoch time (1.5 hours/epoch). N/A means no successful secret recovery.*

LWE parameters		VERDE attack time			
$\log_2 q$	h	*Preprocessing (hrs)*	*Training*	*Total*	(hrs × CPU)
12	8	1.5	2 epochs	4.5	× ???
14	12	2.5	2-5 epochs	5.5-10	× 270
16	14	8.0	2 epochs	11	× ???
18	18	7.0	3 epochs	11.5	× 990
18	20	7.0	1-8 epochs	8.5-19	× ???
20	22	7.5	5 epochs	15	× ???
20	23	7.5	3-4 epochs	12-15	× ???
20	24	7.5	4 epochs	13.5	× ???
20	25	7.5	5 epochs	15	× ???

State of the Art Attack (hrs, 1core)

0.2 (MITM ... in Py)

Implementation in Progress

(Hybrid MITM-Lattice) Models and predictions, exists, but no open source implem.

12 -- 24
(rescaled uSVP)

To summarize the comparison, VERDE is several orders of magnitude behind the state of the art, even on these custom made instances.

The scripts for these two instances are available on the branch

human-LWE

of the leaky-lwe-estimator.

https://github.com/lducas/leaky-LWE-Estimator/tree/human-LWE/human-LWE

< 100 lines of code in total.