SMAUG-T update v4.0

Jung Hee Cheon[1, 2], Hyeongmin Choe[1], Joongeun Choi[4], Dongyeon Hong, Jeongdae Hong[3], Chi-gon Jung[4], Honggoo Kang[4], Janghyeon Lee[4], Seonghyuck Lim[4], Aesun Park[4], Seunghwan Park[4], Jungjoo Seo[2], **Hyoeun Seong**[2], Junbum Shin[2],

[1]Seoul National University, [2]CryptoLab Inc., [3]Ministry of National Defense, [4]Defense Counterintelligence Command

KpqC 9-th workshop

October 23, 2024

SMAUG-T

HEAAN CRYPTO LAB

Defense Counterintelligence Command

SMAUG-T v4.0 was released!
More Secure, More Compact, Less Failure

- SMAUG-T
- Main Updates in SMAUG-T v4.0
- Comparison

SMAUG-T

- Advantages of **MLWE + MLWR**
  - Take both advantages
    - LWE: Conservative security guarantee for key pair
    - LWR: Efficient encryption and decryption
  - **Module structure**: Flexible security level and compact $pk, ctxt$ size
- **Sparse secret key**
  - Compact size of secret key
  - Enables a lower DFP
- **Secure and simple** implementation
  - Power-of-two moduli: Easy implementation of rounding and sampling
  - Discrete Gaussian sampling: Fast and constant-time
  - Sparse CBD: Simple Boolean-based sampling for sparse secret **(v4.0)**

SMAUG-T

- Advantages of **MLWE + MLWR**
  - Take both advantages
    - LWE: Conservative security guarantee for key pair
    - LWR: Efficient encryption and decryption
  - **Module structure**: Flexible security level and compact $pk, ctxt$ size
- **Sparse secret key**
  - Compact size of secret key
  - Enables a lower DFP
- **Secure and simple** implementation
  - Power-of-two moduli: Easy implementation of rounding and sampling
  - Discrete Gaussian sampling: Fast and constant-time
  - Sparse CBD: Simple Boolean-based sampling for sparse secret **(v4.0)**

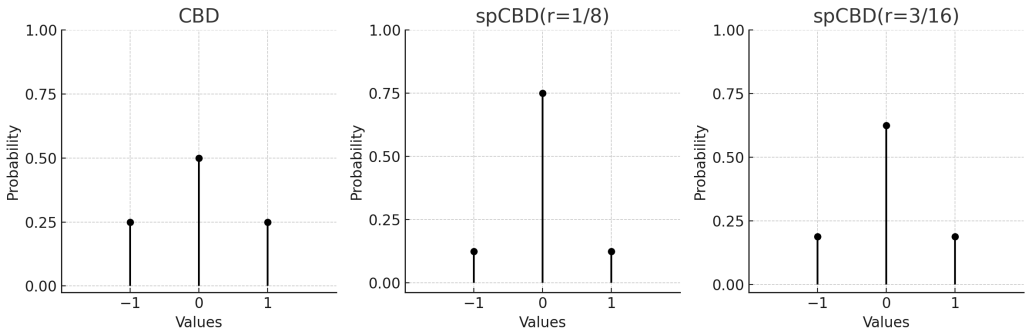
SMAUG-T

- Advantages of **MLWE** + **MLWR**
  - Take both advantages
    - LWE: Conservative security guarantee for key pair
    - LWR: Efficient encryption and decryption
  - **Module structure**: Flexible security level and compact $pk, ctxt$ size
- **Sparse secret key**
  - Compact size of secret key
  - Enables a lower DFP
- **Secure and simple** implementation
  - Power-of-two moduli: Easy implementation of rounding and sampling
  - Discrete Gaussian sampling: Fast and constant-time
  - Sparse CBD: Simple Boolean-based sampling for sparse secret **(v4.0)**

Main updates in SMAUG-T v4.0

New sampler: **sparse CBD**

- **Sparse distribution** sampler for the ephemeral secrets



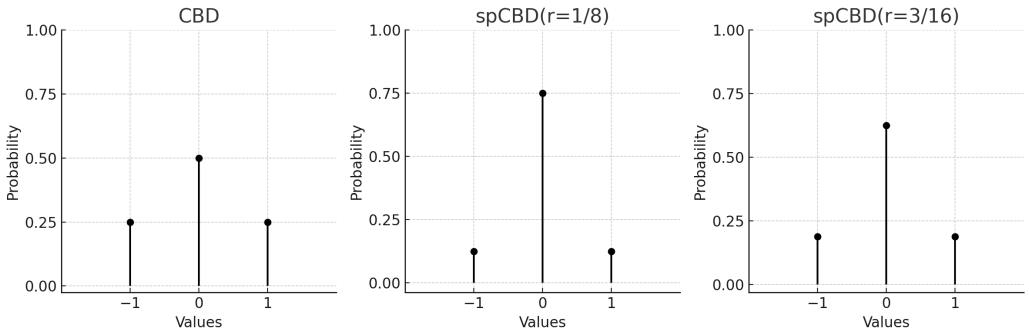
- $\text{spCBD}_{1/8} : \{-1 : 1/8,\ 0 : 3/4,\ 1 : 1/8\}$
- $\text{spCBD}_{3/16} : \{-1 : 3/16,\ 0 : 5/8,\ 1 : 3/16\}$

- **Simple but efficient** sampler based on Boolean operations
  - If the denominator of the r is a power-of-two (2^k), than spCBD_r can be efficiently instantiated by $k+1$ random bits and only the Boolean operations.

Main updates in SMAUG-T v4.0

New sampler: **sparse CBD**

- **Sparse distribution** sampler for the ephemeral secrets



- $\mathsf{spCBD}_{1/8} : \{-1 : 1/8,\ 0 : 3/4,\ 1 : 1/8\}$
- $\mathsf{spCBD}_{3/16} : \{-1 : 3/16,\ 0 : 5/8,\ 1 : 3/16\}$

- **Simple but efficient** sampler based on Boolean operations

- If the denominator of the r is a power-of-two (2^k), than spCBD_r can be efficiently instantiated by $k+1$ random bits and only the Boolean operations.

$\mathsf{spCBD}_{1/8}$:

1: $a, b, c \leftarrow \{0,1\}$
2: $t \leftarrow a \wedge b$
3: $\mathsf{sign} \leftarrow ((c \ll 1) \wedge \mathsf{0x02}) - 1$
4: **return** $t \cdot \mathsf{sign}$

$\mathsf{spCBD}_{3/16}$:

1: $a, b, c, d \leftarrow \{0,1\}$
2: $t \leftarrow a \wedge b \vee c$
3: $\mathsf{sign} \leftarrow ((d \ll 1) \wedge \mathsf{0x02}) - 1$
4: **return** $t \cdot \mathsf{sign}$

Main updates in SMAUG-T v4.0

Parameters sets Security level	TiMER 1	SMAUG-T128 1	SMAUG-T192 3	SMAUG-T256 5
n	256	256	256	256
k	2	2	3	4
(q, p, t)	$(1024, 256, 2)$	$(1024, 256, 2)$	$(2048, 512, 2)$	$(2048, 512, 2)$
p' (compression)	8	32	16	128
h_s (HWT for $\mathbf{s}$)	140	140	264	348
r (spCBD for $\mathbf{r}$)	$1/8$	$1/8$	$1/4$	$3/16$
σ ($\tilde{D}_\sigma$ for errors)	1.0625	1.0625	1.0625	1.0625
Classical core-SVP	119.7	119.7	180.2	250.1
Quantum core-SVP	105.4	105.4	158.6	221.0
Beyond core-SVP	132	132	214	269
Lee et al. [LLW24]*	$(148, 132)$	$(148, 132)$	$(236, 241)$	$(309, 317)$

- **More secure & still efficient**
  - **Parameter update** against improved Meet-LWE [LLW24]
  - Remove memory access to ensure **timing-secure implemenation** considering analysis from Bernstein [Ber24] and TIMECOP [Mor]
    - Constant-time and unbiased HWT sampler [FSL24] in keygen
    - Efficient sparse CBD sampler in encaps/decaps

Main updates in SMAUG-T v4.0

Parameters sets Security level	TiMER 1	SMAUG-T128 1	SMAUG-T192 3	SMAUG-T256 5
Round2 SMAUG-T (v3.0)				
DFP	-132	-120	-136	-167
Public key	672	672	1088	1792
Ciphertext	608	672	1024	1472
New SMAUG-T (v4.0)				
DFP	-161	-118	-179	-194
Public key	672	672	1088	1440
Ciphertext	608	672	992	1376

- **More compact**
  - The sizes of the public keys and ciphertexts are up to 24% smaller than the previous version (already outperforming other lattice-based KEMs)
- **Lower Decryption Failures**
  - The DFP of level 3 and 5 parameters are much smaller than that of the previous version, Kyber [BDK+18], and Saber [DKSRV18]

Main updates in SMAUG-T v4.0

Parameters sets Security level	TiMER 1	SMAUG-T128 1	SMAUG-T192 3	SMAUG-T256 5
Round2 SMAUG-T (v3.0)				
DFP	-132	-120	-136	-167
Public key	672	672	1088	1792
Ciphertext	608	672	1024	1472
New SMAUG-T (v4.0)				
DFP	-161	-118	-179	-194
Public key	672	672	1088	1440
Ciphertext	608	672	992	1376

- **More compact**
  - The sizes of the public keys and ciphertexts are up to 24% smaller than the previous version (already outperforming other lattice-based KEMs)
- **Lower Decryption Failures**
  - The DFP of level 3 and 5 parameters are much smaller than that of the previous version, Kyber [BDK+18], and Saber [DKSRV18]

Comparison: performance

CPU kilocycles and ratio (Intel(R) Core i7-10700K)

Security level		**Cycles (ref)**			**Cycles (AVX2)**		
		SMAUG-T	Kyber		SMAUG-T	Kyber	
1	KeyGen	110	127	(1.2)	38	26	(0.7)
	Encap	100	158	(1.6)	23	38	(1.7)
	Decap	136	187	(1.4)	35	28	(0.8)
3	KeyGen	219	209	(1.0)	57	43	(0.8)
	Encap	204	255	(1.3)	46	65	(1.4)
	Decap	253	286	(1.1)	61	44	(0.7)
5	KeyGen	337	321	(1.0)	77	60	(0.8)
	Encap	334	369	(1.1)	64	79	(1.2)
	Decap	414	414	(1.0)	86	63	(0.7)

*Kyber: `github.com/pq-crystals/kyber` (commit `441c051`)

- In the SMAUG-T parameters, both Toom-Cook and embedded NTT multiplication methods can be used
- **(ref)** shows the results using Toom-Cook, **(AVX2)** provides the results using NTT

Comparison: security, DFP, and size

Security level		SMAUG-T	Kyber	
Security (classical Core-SVP), **DFP** ($\log_2$)				
1	Security	120	118	
	DFP	-118	-139	
3	Security	180	183	
	DFP	-179	-164	
5	Security	250	256	
	DFP	-194	-174	
Sizes (Bytes with ratio)				
1	Pub. key	672	800	(1.2)
	Ctxt.	672	768	(1.1)
3	Pub. key	1,088	1,184	(1.1)
	Ctxt.	992	1,088	(1.1)
5	Pub. key	1,440	1,568	(1.1)
	Ctxt.	1,376	1,568	(1.1)

- The DFP of level 3 and 5 prameters are smaller than that of Kyber
- SMAUG-T has 9%-20% smaller sizes than Kyber

Thank you!

https://kpqc.cryptolab.co.kr/smaug-t

References I

[BDK+18] Joppe Bos, Leo Ducas, Eike Kiltz, T Lepoint, Vadim Lyubashevsky, John M. Schanck, Peter Schwabe, Gregor Seiler, and Damien Stehle.
Crystals - kyber: A cca-secure module-lattice-based kem.
In 2018 IEEE European Symposium on Security and Privacy (EuroS&P), pages 353–367, 2018.

[Ber24] Daniel J. Bernstein.
Timing Attack Against SMAUG-T Software.
Google Groups, KpqC-Bulletin, 2024, 2024.

[DKSRV18] Jan-Pieter D'Anvers, Angshuman Karmakar, Sujoy Sinha Roy, and Frederik 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 10, pages 282–305. Springer, 2018.

[FSL24] Décio Luiz Gazzoni Filho, Tomás S. R. Silva, and Julio López.
Efficient isochronous fixed-weight sampling with applications to NTRU.
Cryptology ePrint Archive, Paper 2024/548, 2024.
https://eprint.iacr.org/2024/548.

References II

[LLW24] Eunmin Lee, Joohee Lee, and Yuntao Wang.
Improved Meet-LWE Attack via Ternary Trees.
Cryptology ePrint Archive, Paper 2024/824, 2024.

[Mor] Moritz Neikes.
TIMECOP.
Artifact available at `https://www.post-apocalyptic-crypto.org/timecop/`.