Introduction to the Security Breakout Session

Rachel Player, Ro Cammarota, Yuriy Polyakov

7th HES Meeting, 13 October 2024

Context

- ISO/IEC JTC1 SC27 standards for BFV/BGV/CKKS/DM/CGGI schemes are under development
- Most are now at committee draft stage

- Standards expected to offer users guidance on choosing parameters or state explicit parameter sets
- For security, relevant to consider concrete hardness of LWE
- Many other parameters relevant when deploying FHE!

- Security Guidelines document referred to in latest ISO/IEC draft
- New version (Oct 2024) of SG document now available! `eprint.iacr.org/2024/463`

Secure LWE parameter sets for FHE in [ACC+19]

distribution	n	security level	logq
(-1, 1)	1024	128	27
		192	19
		256	14
	2048	128	54
		192	37
		256	29
	4096	128	109
		192	75
		256	58
	8192	128	218
		192	152
		256	118
	16384	128	438
		192	305
		256	237
	32768	128	881
		192	611
		256	476

M. R. Albrecht, M. Chase, H. Chen, J. Ding, S. Goldwasser, S. Gorbunov, S. Halevi, J. Hoffstein, K. Laine, K. Lauter, S. Lokam, D. Micciancio, D. Moody, T. Morrison, A. Sahai, V. Vaikuntanathan. Homomorphic encryption standard. eprint.iacr.org/2019/939

Security Guidelines collaboration (eprint.iacr.org/2024/463)

Security Guidelines for Implementing Homomorphic Encryption

Jean-Philippe Bossuat[1], Rosario Cammarota[2], Ilaria Chillotti, Benjamin R. Curtis[4](✉), Wei Dai[5], Huijing Gong[2](✉), Erin Hales[6,7], Duhyeong Kim[2], Bryan Kumara[8], Changmin Lee[9], Xianhui Lu[10], Carsten Maple[8,11], Alberto Pedrouzo-Ulloa[12], Rachel Player[6](✉), Yuriy Polyakov[13], Luis Antonio Ruiz Lopez[14], Yongsoo Song[3], and Donggeon Yhee[15]

[1] Gauss Labs Pte. Ltd.
jeanphilippe.bossuat@gmail.com
[2] Intel Labs
{rosario.cammarota, huijing.gong, duhyeong.kim}@intel.com
[3] Seoul National University
y.song@snu.ac.kr
[4] Zama
ben.curtis@zama.ai
[5] TikTok Inc.
weidai3141@gmail.com
[6] Royal Holloway, University of London
{erin.hales.2018@live.,rachel.player@}rhul.ac.uk
[7] University of Edinburgh
[8] The Alan Turing Institute
{cmaple, bkumara}@turing.ac.uk
[9] Korea Institute for Advanced Study
changminlee@kias.re.kr
[10] Chinese Academy of Sciences
luxianhui@iie.ac.cn
[11] University of Warwick
CM@warwick.ac.uk
[12] atlanTTic, Universidade de Vigo
apedrouzo@gts.uvigo.es
[13] Duality Technologies
ypolyakov@dualitytech.com
[14] Lorica Cybersecurity
luis@loricacyber.com
[15] dgyhee@gmail.com

Keywords: Fully Homomorphic Encryption, Homomorphic Encryption, Learning With Errors, Parameter Selection, Concrete Security, BFV, BGV, CKKS, CGGI, DM

Security Guidelines contributions

1. Present LWE parameter sets that target particular levels of security
   - Security estimated using Lattice Estimator[1]
   - Code: github.com/gong-cr/FHE-Security-Guidelines/
2. Present 'functional' parameter for particular FHE schemes
   - Parameters relevant for security, correctness, and performance
   - Necessarily exemplar!
3. Survey parameter selection support in open source FHE libraries

Several members of the team are here - we welcome feedback!

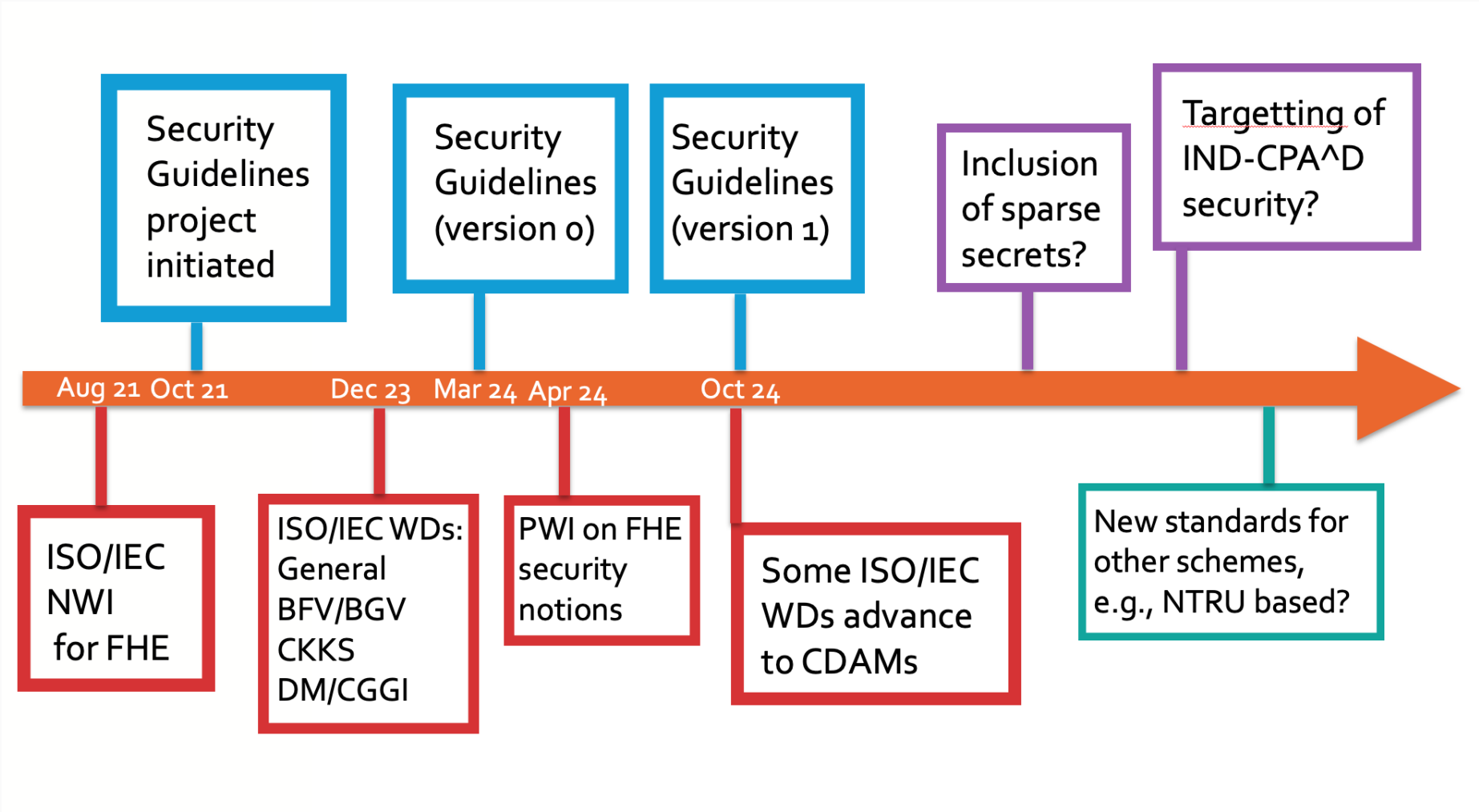
[1] M. R. Albrecht, R. P. and S. Scott. On the concrete hardness of Learning with Errors. In *Journal of Mathematical Cryptology*, 2015. https://github.com/malb/lattice-estimator

Comparison between Security Guidelines and [ACC+19]

[ACC+19]	Security Guidelines
Dimensions $n \in \{1024, ..., 32768\}$	Dimensions $n \in \{1024, ..., 131072\}$
Uniform, ternary, Gaussian secrets No sparse secrets	Binary, ternary, Gaussian secrets Sparse secrets not yet included
Max $\log q$ for fixed σ	Max $\log q$ for fixed n, σ Min $\log \sigma$ for fixed n, q
Not easily reproducible Difficult to update	Code to reproduce all tables Users can re-run code and/or adapt code as needed
Only LWE parameter sets	Examples of comprehensive FHE parameter sets
Describes various FHE schemes	Pointers to schemes and libraries
Describes various LWE algorithms	Pointers to cryptanalysis literature

M. R. Albrecht et al. Homomorphic encryption standard. eprint.iacr.org/2019/939
J.-P. Bossuat et al. Security Guidelines for Implementing Homomorphic Encryption eprint.iacr.org/2024/463

Roadmap for ISO/IEC standards and Security Guidelines



Goals of the Security Breakout Session today

- This will be a working session!
- We will assume some prior knowledge of FHE security

- We will produce written outputs on two topics:
  - Parameter sets with sparse secrets
  - IND-CPA^D security

- These written outputs will be shared with Security Guidelines authors to inform subsequent versions of this document

Structure of the Security Breakout Session today

- **Opening** (14:00 - 14:30)
  - We will gather concrete questions to be addressed in the outputs
  - We have prepared some suggested questions
  - We encourage participants to suggest additional questions, and provide input to the discussion via short presentations

- **Discussions** (14:30 - 16:00)
  - We will discuss key issues to address the identified questions
  - We may split into smaller groups to address particular questions
  - We will collaborate in Overleaf to capture the discussion

- **Wrap up** (16:00 - 16:40)
  - We will edit the notes captured to produce the written outputs