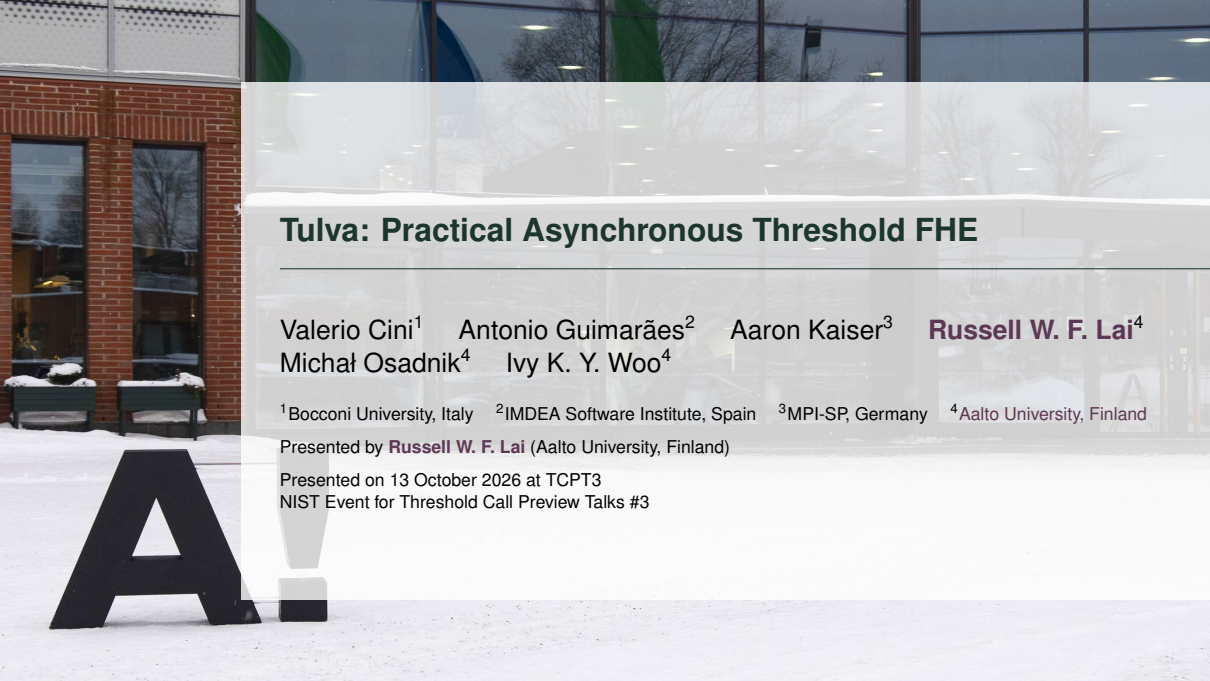


Tulva: Practical Asynchronous Threshold FHE

Valerio Cini[1] Antonio Guimarães[2] Aaron Kaiser[3] **Russell W. F. Lai**[4]
Michał Osadnik[4] Ivy K. Y. Woo[4]

[1]Bocconi University, Italy [2]IMDEA Software Institute, Spain [3]MPI-SP, Germany [4]Aalto University, Finland

Presented by **Russell W. F. Lai** (Aalto University, Finland)

Presented on 13 October 2026 at TCPT3
NIST Event for Threshold Call Preview Talks #3

The team

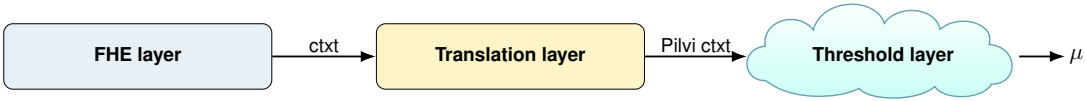


Aalto University	**Russell W. F. Lai**, Michał Osadnik, Ivy K. Y. Woo
Bocconi University	Valerio Cini
IMDEA Software Institute	Antonio Guimarães
MPI-SP	Aaron Kaiser

Tulva: generic compiler from FHE to threshold FHE

Tulva [CGLOW27]

any FHE scheme $\longmapsto$ asynchronous threshold FHE scheme



- † instantiable from any FHE scheme without modification
- † Setup, Enc, Eval taken black-box
- † inherit optimisations of FHE

- † bootstrap and key switch
- † public and deterministic
- † can be preprocessed by evaluator
- † decouples parameter choice of the two layers

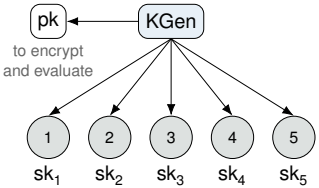
- † adapted from Pilvi [CLW25]
- † flexible threshold profile
- † asynchronous decryption
- † small partial decryptions: one ring element

[CLW25] Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. “Pilvi: Lattice Threshold PKE with Small Decryption Shares and Improved Security”. In: *ASIACRYPT 2025, Part VI*. 2025

[CGLOW27] Valerio Cini, Antonio Guimarães, Russell W. F. Lai, Michał Osadnik, and Ivy K. Y. Woo. “Tulva: Practical Asynchronous Threshold FHE”. In: *2027 IEEE Symposium on Security and Privacy*. 2027

Threshold fully homomorphic encryption

KGen: **a public key, and the secret key shared among $n = 5$**



KGen by a trusted dealer; a DKG could replace it (out of scope of this package)

Any $k = 3$ of them decrypt any ciphertext

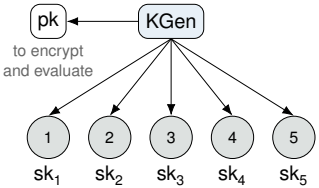
Fewer than $k = 3$ keys and partial decryptions: nothing

Example

Threshold profile: $k = 3$ out of $n = 5$

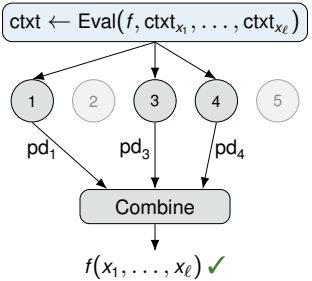
Threshold fully homomorphic encryption

KGen: **a public key, and the secret key shared among $n = 5$**



KGen by a trusted dealer; a DKG could replace it (out of scope of this package)

Any $k = 3$ of them decrypt any ciphertext



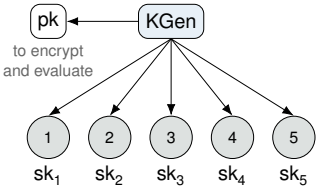
Fewer than $k = 3$ keys and partial decryptions: nothing

Example

Threshold profile: $k = 3$ out of $n = 5$

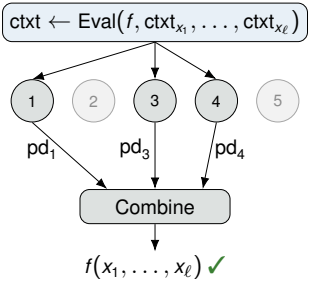
Threshold fully homomorphic encryption

KGen: **a public key, and the secret key shared among $n = 5$**

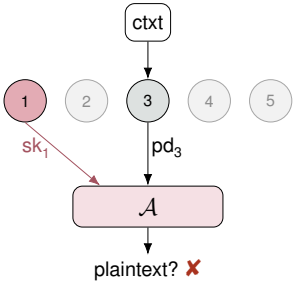


KGen by a trusted dealer; a DKG could replace it (out of scope of this package)

Any $k = 3$ of them decrypt any ciphertext



Fewer than $k = 3$ keys and partial decryptions: nothing



Example

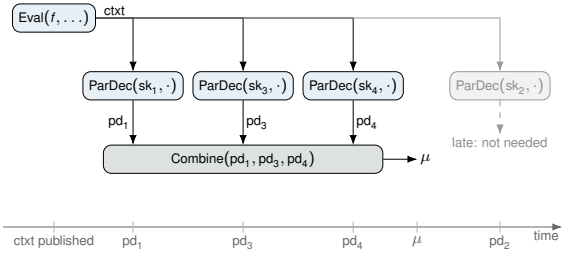
Threshold profile: $k = 3$ out of $n = 5$

Asynchronous threshold decryption

Non-interactive threshold decryption

† $\mathsf{pd}_i \leftarrow \mathsf{ParDec}(\mathsf{pk}, \mathsf{sk}_i, \mathsf{ctxt})$
To be run locally by each partial decryptor

† $\mu \leftarrow \mathsf{Combine}(\mathsf{pk}, T, (\mathsf{pd}_i)_{i \in T}, \mathsf{ctxt})$
Recover message from any k partial decryptions



Asynchrony: no coordination

† no coordination between partial decryptors

† combiner collects partial decryptions from any k parties in any order

† partial decryptors need not be online together

Network

† authenticated channel between each pair of communicating parties

† no broadcast channel

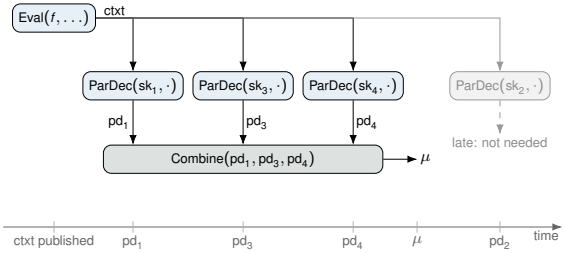
† delays and drops only affect liveness, not security

Asynchronous threshold decryption

Non-interactive threshold decryption

† $\mathsf{pd}_i \leftarrow \mathsf{ParDec}(\mathsf{pk}, \mathsf{sk}_i, \mathsf{ctxt})$
To be run locally by each partial decryptor

† $\mu \leftarrow \mathsf{Combine}(\mathsf{pk}, T, (\mathsf{pd}_i)_{i \in T}, \mathsf{ctxt})$
Recover message from any k partial decryptions



Asynchrony: no coordination

† no coordination between partial decryptors

† combiner collects partial decryptions from any k parties in any order

† partial decryptors need not be online together

Network

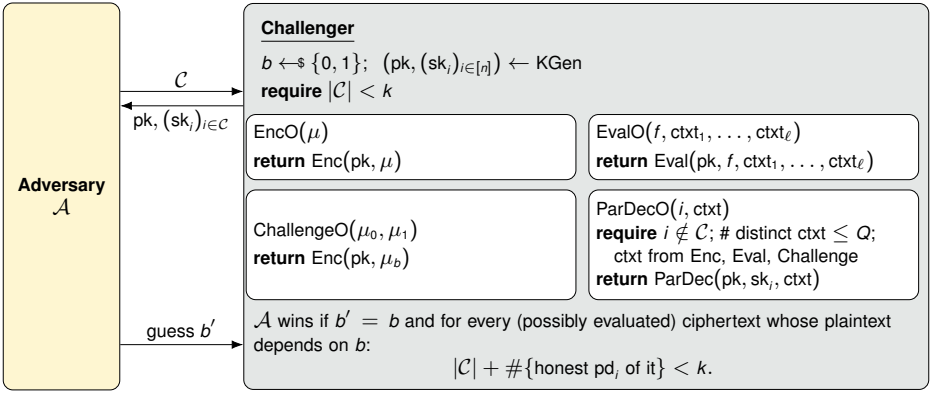
† authenticated channel between each pair of communicating parties

† no broadcast channel

† delays and drops only affect liveness, not security

Security model: Q-bounded IND-CPA

Challenge messages stay hidden even after some partial decryptions of challenge ciphertexts.
(Adopted from [CLW25; BKW26].)



[CLW25] Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. “Pilvi: Lattice Threshold PKE with Small Decryption Shares and Improved Security”. In: *ASIACRYPT 2025, Part VI*. 2025

[BKW26] Chris Brzuska, Michael Klooß, and Ivy K. Y. Woo. “Threshold Public-Key Encryption: Definitions, Relations, and CPA-to-CCA Transforms”. In: *PKC 2026, Part IV*. 2026

Why reveal partial decryptions of challenge ciphertexts?

Useful when using threshold FHE to build other threshold primitives.

Example: Signature + (async.) threshold FHE $\longmapsto$ (async.) threshold signature [BGGJKRS18]

Keys: $(\mathsf{vk}, \mathsf{sk}_{\mathsf{SIG}}) \leftarrow \mathsf{SIG.KGen}$; publish vk and $\mathsf{ctxt}_{\mathsf{sk}} \leftarrow \mathsf{Enc}(\mathsf{pk}, \mathsf{sk}_{\mathsf{SIG}})$; shareholder i keeps sk_i.

Sign m**:** $\mathsf{ctxt}_{\mathsf{sk}} \to \mathsf{Eval}(\mathsf{SIG.Sign}(\cdot, m)) \xrightarrow{\mathsf{ctxt}_\sigma} \mathsf{ParDec}(\mathsf{sk}_i, \cdot) \xrightarrow[\text{partial signature}]{\mathsf{pd}_i} \mathsf{Combine} \to \sigma$

Verify: $\mathsf{SIG.Vf}(\mathsf{vk}, m, \sigma)$.

† [BCKMTZ22] defined a hierarchy of threshold signature security levels TS-UF-0, TS-UF-1, . . . , TS-UF-4.

† TS-UF-1 security: no forgery on m given $< k - |\mathcal{C}|$ honest partial signatures on m.

† To achieve TS-UF-1 or above, threshold FHE must stay secure even after partial decryptions of the challenge.

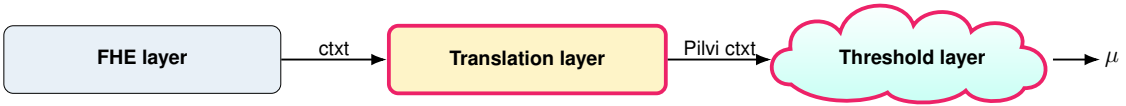
[BGGJKRS18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. "Threshold Cryptosystems from Threshold Fully Homomorphic Encryption". In: *CRYPTO 2018, Part I*. 2018

[BCKMTZ22] Mihir Bellare, Elizabeth C. Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. "Better than Advertised Security for Non-interactive Threshold Signatures". In: *CRYPTO 2022, Part IV*. 2022

Tulva: generic compiler from FHE to threshold FHE

Tulva [CGLOW27]

any FHE scheme $\longmapsto$ asynchronous threshold FHE scheme



[CGLOW27] Valerio Cini, Antonio Guimarães, Russell W. F. Lai, Michał Osadnik, and Ivy K. Y. Woo. "Tulva: Practical Asynchronous Threshold FHE". In: *2027 IEEE Symposium on Security and Privacy*. 2027

Threshold layer: Pilvi, threshold PKE with small decryption shares

Pilvi [CLW25] (simplified)

Regev's PKE over module lattices, with a Shamir-shared secret key

Keys

$\mathsf{pk} = \left(\mathbf{A},\ \mathbf{b}^\mathsf{T} = \mathbf{r}^\mathsf{T}\mathbf{A} + \mathbf{e}^\mathsf{T}\right)$
shareholder i gets $\mathbf{s}_i$, a Shamir share of $\mathbf{r}$

Encryption

$\mathbf{c}_0 = \mathbf{A}\mathbf{x}, \quad c_1 = \mathbf{b}^\mathsf{T}\mathbf{x} + \lfloor q/p \rceil \cdot \mu$
with $\mathbf{x}$ short

ParDec

$\mathsf{pd}_i = \mathbf{s}_i^\mathsf{T}\mathbf{c}_0 + e_i \in \mathcal{R}_q$
with masking noise e_i

Combine

$\sum_{i \in T} \lambda_{T,i}\, \mathsf{pd}_i = \mathbf{r}^\mathsf{T}\mathbf{c}_0 + \sum_{i \in T} \lambda_{T,i}\, e_i$
then round $c_1 - (\ldots)$ to μ

The usual obstacle

Shamir sharing uses a Vandermonde matrix $\mathbf{V}$. In the lattice setting, both $\mathbf{V}$ and $\mathbf{V}^{-1}$ need to be low norm:

- † Construction, $\mathbf{V}^{-1}$: the Lagrange coefficients $\lambda_{T,i}$ in Combine scale the masking noise e_i.
- † Security proof, $\mathbf{V}$ and $\mathbf{V}^{-1}$: the proof first recovers from simulated partial decryptions ($\mathbf{V}^{-1}$), then re-derives the honest ones ($\mathbf{V}$); both steps scale their noise.

Over $\mathcal{R}_q$, $\mathbf{V}^{-1}$ is typically not short.

Threshold layer: Pilvi, threshold PKE with small decryption shares

Pilvi [CLW25] (simplified)

Regev's PKE over module lattices, with a Shamir-shared secret key

Keys

$\mathsf{pk} = \left(\mathbf{A},\ \mathbf{b}^\mathsf{T} = \mathbf{r}^\mathsf{T}\mathbf{A} + \mathbf{e}^\mathsf{T}\right)$
shareholder i gets $\mathbf{s}_i$, a Shamir share of $\mathbf{r}$

Encryption

$\mathbf{c}_0 = \mathbf{A}\mathbf{x}, \quad c_1 = \mathbf{b}^\mathsf{T}\mathbf{x} + \lfloor q/p \rceil \cdot \mu$
with $\mathbf{x}$ short

ParDec

$\mathsf{pd}_i = \mathbf{s}_i^\mathsf{T}\mathbf{c}_0 + e_i \in \mathcal{R}_q$
with masking noise e_i

Combine

$\sum_{i \in T} \lambda_{T,i}\, \mathsf{pd}_i = \mathbf{r}^\mathsf{T}\mathbf{c}_0 + \sum_{i \in T} \lambda_{T,i}\, e_i$
then round $c_1 - (\ldots)$ to μ

The usual obstacle

Shamir sharing uses a Vandermonde matrix $\mathbf{V}$. In the lattice setting, both $\mathbf{V}$ and $\mathbf{V}^{-1}$ need to be low norm:

- † Construction, $\mathbf{V}^{-1}$: the Lagrange coefficients $\lambda_{T,i}$ in Combine scale the masking noise e_i.
- † Security proof, $\mathbf{V}$ and $\mathbf{V}^{-1}$: the proof first recovers from simulated partial decryptions ($\mathbf{V}^{-1}$), then re-derives the honest ones ($\mathbf{V}$); both steps scale their noise.

Over $\mathcal{R}_q$, $\mathbf{V}^{-1}$ is typically not short.

Subtractive sets: Shamir sharing over cyclotomic rings

ξ-subtractive set [AL21; KLNO24]

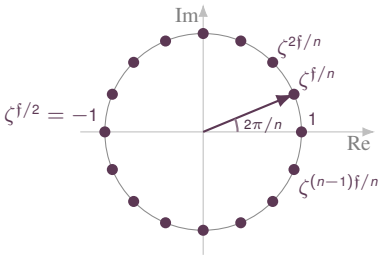
A set $\Xi \subset \mathcal{R}$ of n evaluation points is *ξ-subtractive* if

$$\xi \cdot \mathbf{V}_T^{-1} \in \mathcal{R}^{k \times k}$$

for every size-k subset $T \subseteq \Xi$, where $\mathbf{V}_T$ is the Vandermonde matrix with rows $(1, \nu, \ldots, \nu^{k-1})$, $\nu \in T$.

Our set

$$\Xi = \{1,\ \zeta^{\mathfrak{f}/n},\ \zeta^{2\mathfrak{f}/n},\ \ldots,\ \zeta^{(n-1)\mathfrak{f}/n}\}$$
in $\mathcal{R} = \mathbb{Z}[\zeta]$, with $\mathfrak{f}$ a power of two and $n \mid \mathfrak{f}$
$$\xi = 2^{\lceil \log_2 k \rceil} \approx k$$



Ξ for $n = 16$.

[AL21] Martin R. Albrecht and Russell W. F. Lai. "Subtractive Sets over Cyclotomic Rings - Limits of Schnorr-Like Arguments over Lattices". In: *CRYPTO 2021, Part II*. 2021

[KLNO24] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik. "RoK, Paper, SISsors Toolkit for Lattice-Based Succinct Arguments - (Extended Abstract)". In: *ASIACRYPT 2024, Part V*. 2024

Cost versus threshold profile

In principle, Pilvi/Tulva support any profile (k, n):

- † **V** is short: it consists of roots of unity.
- † $\xi \cdot \mathbf{V}_T^{-1} \in \mathcal{R}^{k \times k}$, independent of q. We can pick q large enough to make it "short".

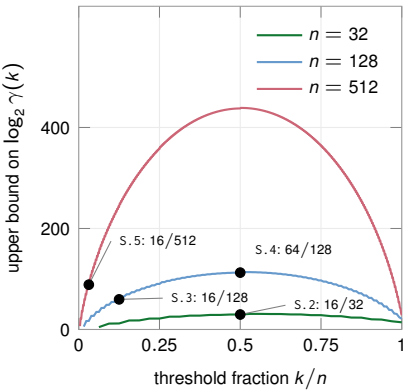
Concretely, costs depend heavily on the modulus q. Roughly,

$$q \approx n^{O(\min(k, n-k))}.$$

For example, we need $q \gg \gamma(k)$ where

$$\gamma(k) := \max_{T \subseteq \Xi,\, |T| = k-1} \left\| \xi \cdot \mathbf{V}_\Xi \cdot \mathbf{V}_{\{0\} \cup T}^{-1} \right\|_{2,2}$$

Cost versus threshold profile



In principle, Pilvi/Tulva support any profile (k, n):

- † $\mathbf{V}$ is short: it consists of roots of unity.
- † $\xi \cdot \mathbf{V}_T^{-1} \in \mathcal{R}^{k \times k}$, independent of q. We can pick q large enough to make it "short".

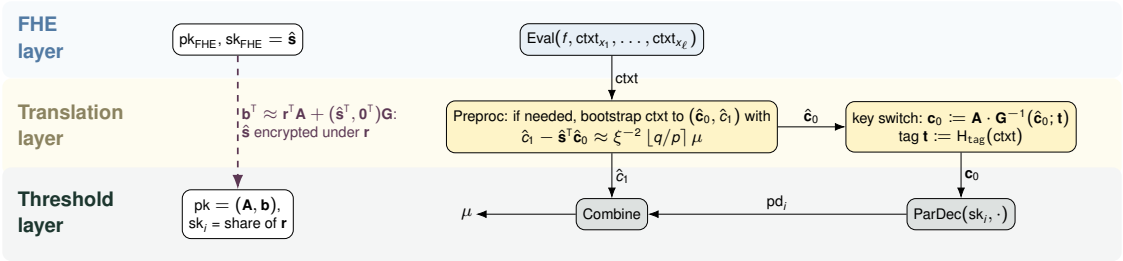
Concretely, costs depend heavily on the modulus q. Roughly,

$$q \approx n^{O(\min(k, n-k))}.$$

For example, we need $q \gg \gamma(k)$ where

$$\gamma(k) := \max_{T \subseteq \Xi,\, |T| = k-1} \left\| \xi \cdot \mathbf{V}_\Xi \cdot \mathbf{V}_{\{0\} \cup T}^{-1} \right\|_{2,2}$$

Translation layer: from any FHE ciphertext to a Pilvi ciphertext



Preproc and key switch:

- The only scheme-specific step.
- Preproc skipped if Eval already outputs a ciphertext of this form.
- Public and deterministic. Delegable e.g. to the server that ran Eval.

Security

Theorem

Assume that FHE is IND-CPA secure and MLWE [LS15] holds.
Then Tulva[FHE] is Q-bounded IND-CPA secure in the random oracle model.

Proof part 1: threshold layer (adapted from Pilvi)

- By MLWE, key-switching key **b** is uniform.
- By the Vandermonde structure and fewer than $k - |\mathcal{C}|$ honest partial decryptions, challenge partial decryptions become uniform.
- New: the (pseudo)random tag **t** rerandomises the translated Pilvi ciphertext.

Proof part 2: FHE layer

- Other partial decryptions are simulated via linear decryption, from the leakage of an IND-CPA-with-leakage game of the base scheme.
- By noise flooding with the masking noise, IND-CPA implies this game (*tulva* is Finnish for *flood*).

[LS15] Adeline Langlois and Damien Stehlé. “Worst-case to average-case reductions for module lattices”. In: *DCC* (2015)

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. “Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds”. In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Preliminary performance of `tulva-tfhe`: TFHE compiled by Tulva

Since Tulva is a generic compiler, we measure performance by its decryption overhead. Performance of Enc and Eval is inherited from base FHE. We use TFHE with [CGGI16] bootstrapping as an example.

Set	k/n	q	$\lvert\mu\rvert$ [bit]	$\lvert$pk$\rvert$ [kB]	$\lvert$pd$\rvert$ [kB]	Preproc [s]	ParDec [ms]	Combine [µs]
S.1	4/8	2^{210}	4 | 1024	1083	0.7	0.13 | 5.83	0.64 | 0.51	39 | 39
S.2	16/32	2^{235}	4 | 1024	1432	1.0	0.16 | 7.70	0.60 | 0.43	91 | 77
S.3	16/128	2^{300}	4 | 1024	3038	2.0	0.24 | 12.68	1.11 | 0.77	94 | 82
S.4	64/128	2^{329}	4 | 1024	4750	2.5	0.36 | 22.58	2.80 | 2.98	223 | 610
S.5	16/512	2^{368}	4 | 1024	6624	3.0	0.47 | 31.03	3.68 | 4.26	534 | 562
L.1	4/8	2^{215}	8192	1613	5.8	74.17	0.63	70
L.2	16/32	2^{240}	8192	1800	8.5	80.08	0.34	403
L.3	16/128	2^{308}	8192	4312	16.8	144.95	0.62	967
L.4	64/128	2^{336}	8192	5880	20.5	258.87	1.25	1495
L.5	16/512	2^{376}	8192	7520	24.8	303.27	1.10	875

At least 128-bit security, $Q = 2^{64}$, $p = 2^4$, ring degree $\varphi = 256$ (S) or 2048 (L). AWS `c7a.32xlarge`.

(Includes optimisations made after the preview write-up.)

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. "Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds". In: *ASIACRYPT 2016, Part I*. 2016

Handling malicious partial decryptions: Tulva$^+$

Tulva does not check integrity of partial decryptions: one incorrect pd_i can shift the output undetectably.

Tulva$^+$

- † At least **security with abort**: honest combiner outputs correct message or aborts.
- † Possibly **robustness**: honest combiner recovers correct message from any k correct partial decryptions.

Three candidate approaches:

Approach	Idea	Guarantee	Cost
1. Proofs of integrity	each pd_i carries a ZK proof of correctness	robustness	larger, slower pd_i
2. Homomorphic authentication	Preproc also evaluates a MAC or signature; μ is released only if the recovered tag is valid	with abort	slower Preproc
3. Consistency check	collect $2k-1$ partial decryptions; μ is released only if they are consistent	with abort	honest majority

Approaches 2 and 3 assume confidential channels between partial decryptors and the combiner. After an abort in approach 2 or 3: request proofs of integrity, exclude failing shareholders, retry.

Handling malicious partial decryptions: Tulva$^+$

Tulva does not check integrity of partial decryptions: one incorrect pd_i can shift the output undetectably.

Tulva$^+$

- † At least **security with abort**: honest combiner outputs correct message or aborts.
- † Possibly **robustness**: honest combiner recovers correct message from any k correct partial decryptions.

Three candidate approaches:

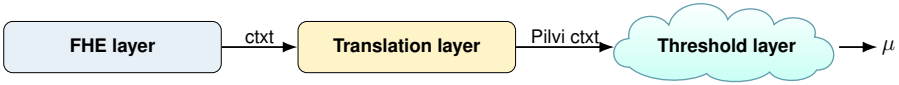
Approach	Idea	Guarantee	Cost
1. Proofs of integrity	each pd_i carries a ZK proof of correctness	robustness	larger, slower pd_i
2. Homomorphic authentication	Preproc also evaluates a MAC or signature; μ is released only if the recovered tag is valid	with abort	slower Preproc
3. Consistency check	collect $2k-1$ partial decryptions; μ is released only if they are consistent	with abort	honest majority

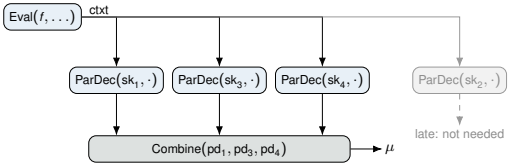
Approaches 2 and 3 assume confidential channels between partial decryptors and the combiner. After an abort in approach 2 or 3: request proofs of integrity, exclude failing shareholders, retry.

Summary

Tulva

A compiler from essentially any FHE scheme to an asynchronous threshold FHE scheme.





Fast: threshold decryption in milliseconds, after public preprocessing.

Flexible: any (k, n), including dishonest majority.

Secure: Q-bounded IND-CPA, even given partial decryptions of challenge ciphertexts.

Pilvi	[CLW25], ASIACRYPT 2025
Tulva	[CGLOW27], IEEE S&P 2027
Team	Valerio Cini, Antonio Guimarães, Aaron Kaiser, **Russell W. F. Lai**, Michał Osadnik, Ivy K. Y. Woo
Contact	`tulva-threshold-fhe@googlegroups.com`

Thank you!

Backup: the threshold layer in formulas

KGen: an FHE layer and a threshold layer

Keep $(\mathsf{pk}_{\mathsf{FHE}}, \hat{\mathbf{s}})$. Publish an MLWE-masked, gadget-encoded copy of $\hat{\mathbf{s}}$ under a fresh secret $\mathbf{r}$:

$$\mathbf{b}^{\mathsf{T}} \coloneqq \mathbf{r}^{\mathsf{T}}\mathbf{A} + \mathbf{e}^{\mathsf{T}} + (\hat{\mathbf{s}}^{\mathsf{T}}, \mathbf{0}^{\mathsf{T}})\,\mathbf{G}_{\beta,q} \bmod q, \qquad \mathbf{A} \coloneqq \mathsf{H}_{\mathsf{pk}}(\mathsf{seed}), \qquad \mathsf{pk} \coloneqq (\mathsf{pk}_{\mathsf{FHE}}, \mathbf{A}, \mathbf{b}).$$

Shareholder i receives $\mathsf{sk}_i \coloneqq \mathbf{s}_i$, the Shamir share of $\mathbf{r}$ at evaluation point $\zeta^{i\hat{\mathsf{f}}/n} \in \Xi$, scaled by ξ.

$\mathsf{ParDec}(\mathsf{pk}, \mathsf{sk}_i, \mathsf{ctxt})$: local, one ring element

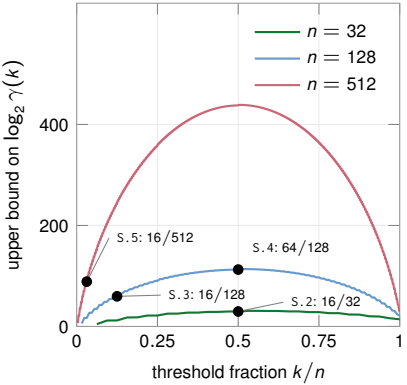
Decompose the tagged, preprocessed ciphertext, $\mathbf{x} \coloneqq \mathbf{G}^{-1}_{\beta,q}(\hat{\mathbf{c}}_0; \mathsf{H}_{\mathsf{tag}}(\mathsf{ctxt}))$.
Output $\mathsf{pd}_i \coloneqq \mathbf{s}_i^{\mathsf{T}}(\mathbf{A}\mathbf{x}) + e_i \bmod q \in \mathcal{R}_q$.

$\mathsf{Combine}(\mathsf{pk}, T, (\mathsf{pd}_i)_{i\in T}, \mathsf{ctxt})$: public

Reconstruct $y \coloneqq \xi\,\mathbf{v}_0^{\mathsf{T}}\mathbf{V}_T^{-1}(\mathsf{pd}_i)_{i\in T} \approx \xi^2\,\mathbf{r}^{\mathsf{T}}\mathbf{A}\mathbf{x}$, where $\mathbf{v}_0 \coloneqq (1; 0; 0; \ldots; 0)$.
Output $\left\lfloor \frac{p}{q}\left(\xi^2\hat{c}_1 - \xi^2\mathbf{b}^{\mathsf{T}}\mathbf{x} + y\right)\right\rceil \bmod p = \mu$.

The gadget term cancels $\hat{\mathbf{s}}^{\mathsf{T}}\hat{\mathbf{c}}_0$, the reconstruction cancels $\mathbf{r}^{\mathsf{T}}\mathbf{A}\mathbf{x}$, and what is left is $\lfloor q/p \rceil \cdot \mu$ plus noise, small because $\mathbf{x}$ is short and $\xi \cdot \mathbf{V}_T^{-1}$ has short entries in $\mathcal{R}$.

Backup: quality of the evaluation points



Bound, adapted from [KLLPS26]

For $2 \le k \le n$ and $\xi = 2^{\lceil \log_2 k \rceil}$:

$$\gamma(k) \le \xi \sqrt{(n-k+1)(A^2 + (k-1)B^2) + 1}$$

where

$$A = 2^{k-1} \prod_{j=1}^{\lfloor (k-2)/2 \rfloor} \cos^2(\pi j/n)$$

$$B = \prod_{j=1}^{\lfloor (k-3)/2 \rfloor} \cos^2(\pi j/n) \cdot \prod_{j=1}^{\lfloor (k-1)/2 \rfloor} \sin^{-2}(\pi j/n)$$

[KLLPS26] Won Kim, Changmin Lee, JeongHwan Lee, Alain Passelègue, and Damien Stehlé. “Asynchronous Lagrange-Based Threshold FHE with Smaller Modulus Overhead”. In: *CRYPTO 2026*. 2026

References I

[AL21] Martin R. Albrecht and Russell W. F. Lai. “Subtractive Sets over Cyclotomic Rings - Limits of Schnorr-Like Arguments over Lattices”. In: *CRYPTO 2021, Part II*. 2021.

[BCKMTZ22] Mihir Bellare, Elizabeth C. Crites, Chelsea Komlo, Mary Maller, Stefano Tessaro, and Chenzhi Zhu. “Better than Advertised Security for Non-interactive Threshold Signatures”. In: *CRYPTO 2022, Part IV*. 2022.

[BGGJKRS18] Dan Boneh, Rosario Gennaro, Steven Goldfeder, Aayush Jain, Sam Kim, Peter M. R. Rasmussen, and Amit Sahai. “Threshold Cryptosystems from Threshold Fully Homomorphic Encryption”. In: *CRYPTO 2018, Part I*. 2018.

[BKW26] Chris Brzuska, Michael Klooß, and Ivy K. Y. Woo. “Threshold Public-Key Encryption: Definitions, Relations, and CPA-to-CCA Transforms”. In: *PKC 2026, Part IV*. 2026.

[CGGI16] Ilaria Chillotti, Nicolas Gama, Mariya Georgieva, and Malika Izabachène. “Faster Fully Homomorphic Encryption: Bootstrapping in Less Than 0.1 Seconds”. In: *ASIACRYPT 2016, Part I*. 2016.

References II

[CGLOW27] Valerio Cini, Antonio Guimarães, Russell W. F. Lai, Michał Osadnik, and Ivy K. Y. Woo. “Tulva: Practical Asynchronous Threshold FHE”. In: *2027 IEEE Symposium on Security and Privacy*. 2027.

[CLW25] Valerio Cini, Russell W. F. Lai, and Ivy K. Y. Woo. “Pilvi: Lattice Threshold PKE with Small Decryption Shares and Improved Security”. In: *ASIACRYPT 2025, Part VI*. 2025.

[KLLPS26] Won Kim, Changmin Lee, JeongHwan Lee, Alain Passelègue, and Damien Stehlé. “Asynchronous Lagrange-Based Threshold FHE with Smaller Modulus Overhead”. In: *CRYPTO 2026*. 2026.

[KLNO24] Michael Klooß, Russell W. F. Lai, Ngoc Khanh Nguyen, and Michal Osadnik. “RoK, Paper, SISsors Toolkit for Lattice-Based Succinct Arguments - (Extended Abstract)”. In: *ASIACRYPT 2024, Part V*. 2024.

[LS15] Adeline Langlois and Damien Stehlé. “Worst-case to average-case reductions for module lattices”. In: *DCC* (2015).