On Algebraic Homomorphic Encryption and its Applications to Doubly-Efficient PIR

Hiroki Okada[1], Rachel Player[2],
Simon Pohmann[2], Christian Weinert[2]

[1] KDDI Research and The University of Tokyo, Japan

[2] Royal Holloway, University of London, UK

Some slides adapted from slides of Simon Pohmann

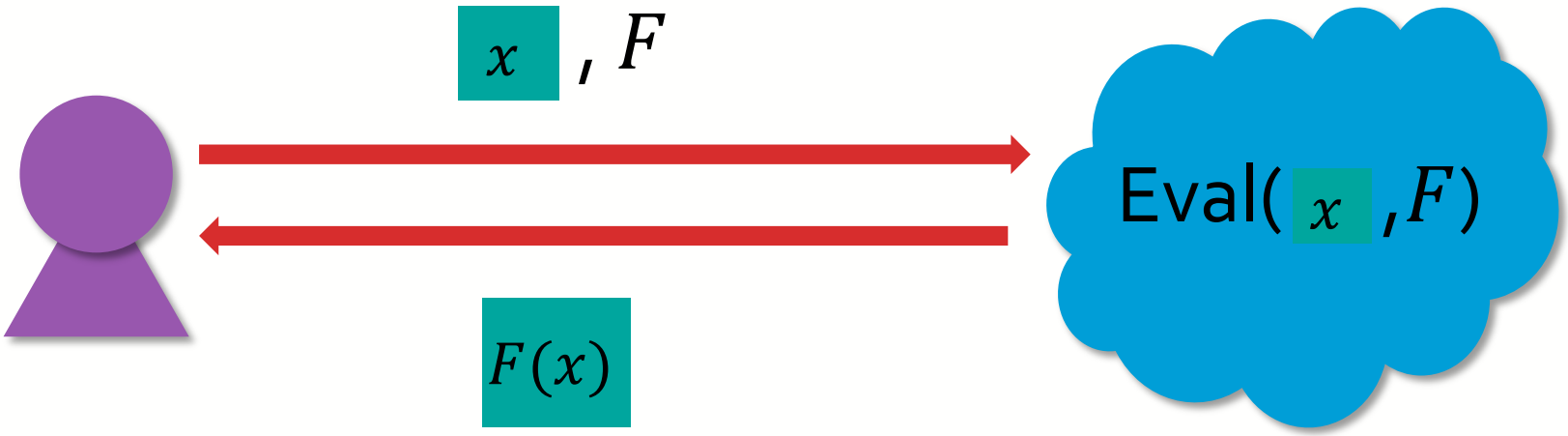
KDDI Research

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Background and prior work

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Homomorphic encryption

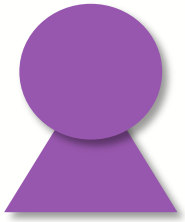


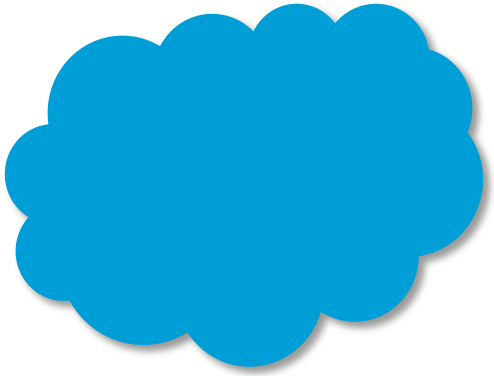
- Client can outsource computation of $F(x)$ on their data x
- Server does not learn x or $F(x)$

x : Encryption of x

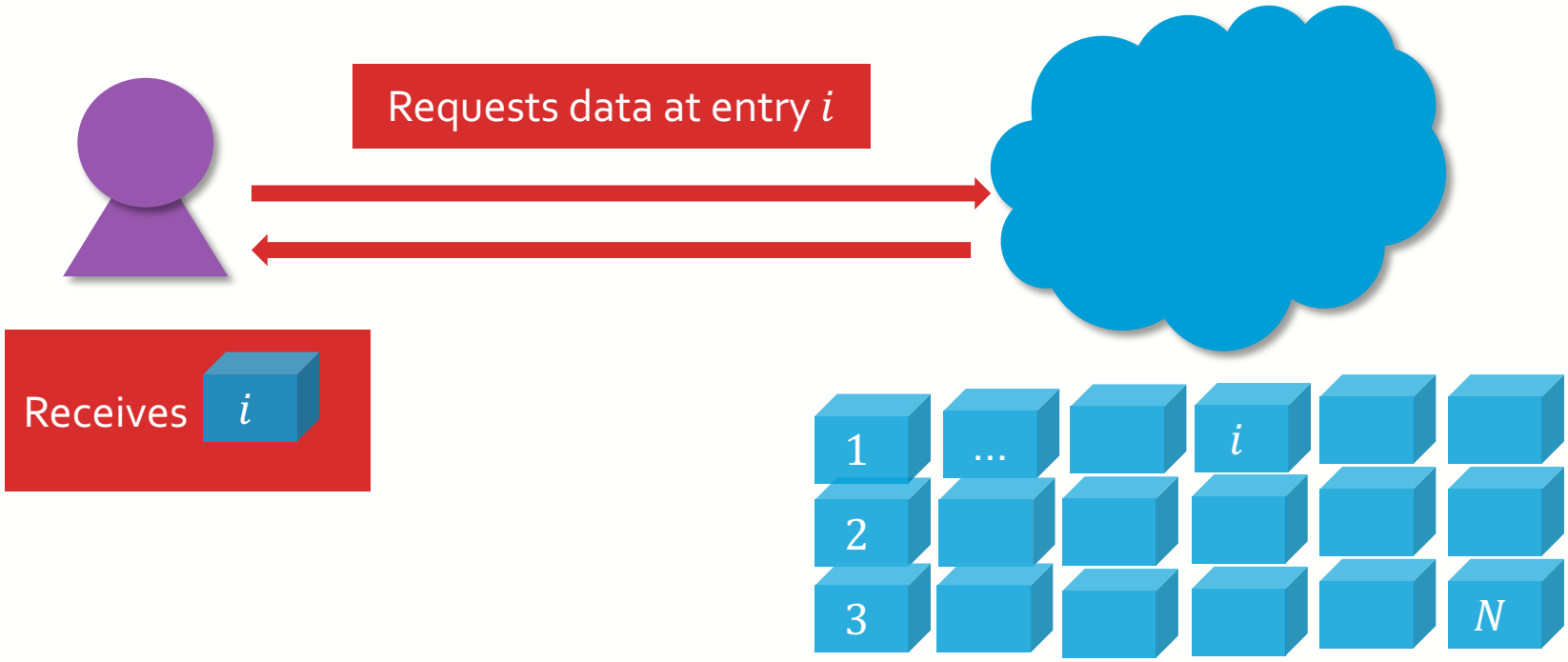
F(x) : Encryption of $F(x)$

Private Information Retrieval (PIR)

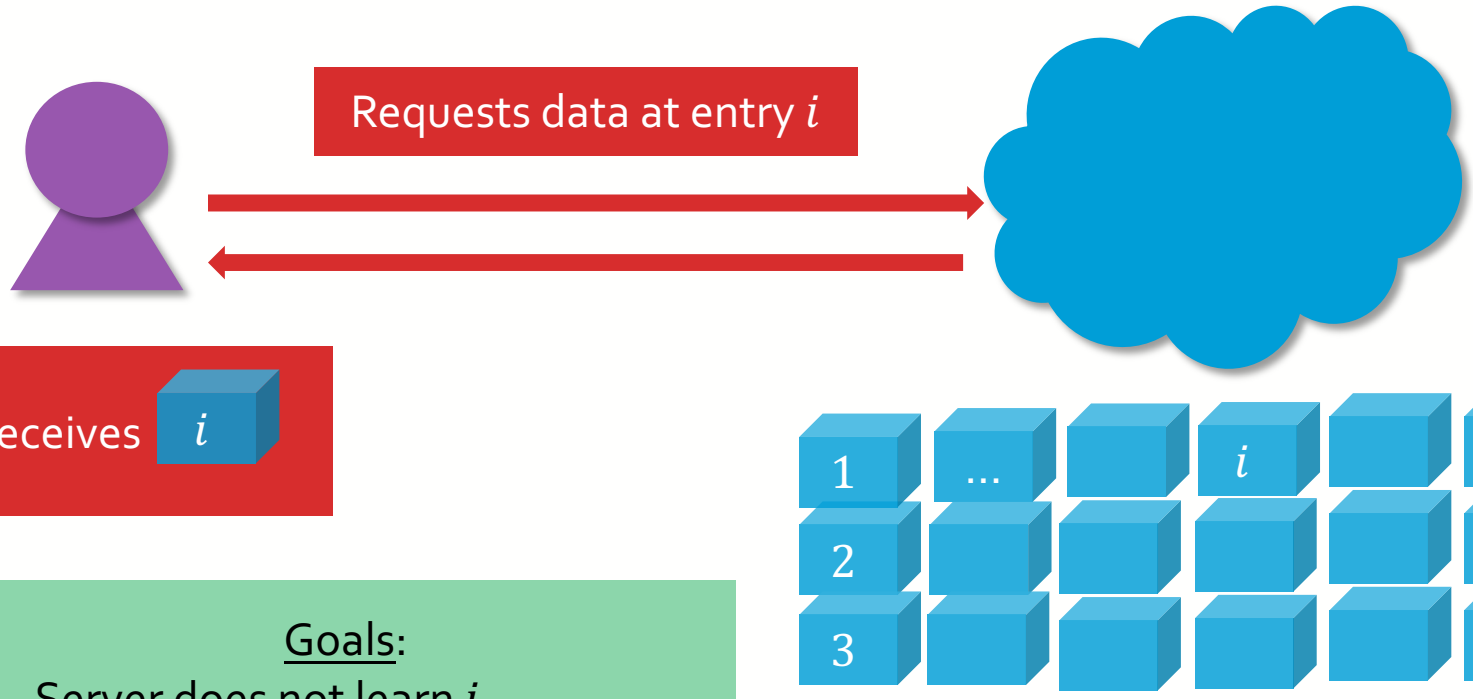




Private Information Retrieval (PIR)



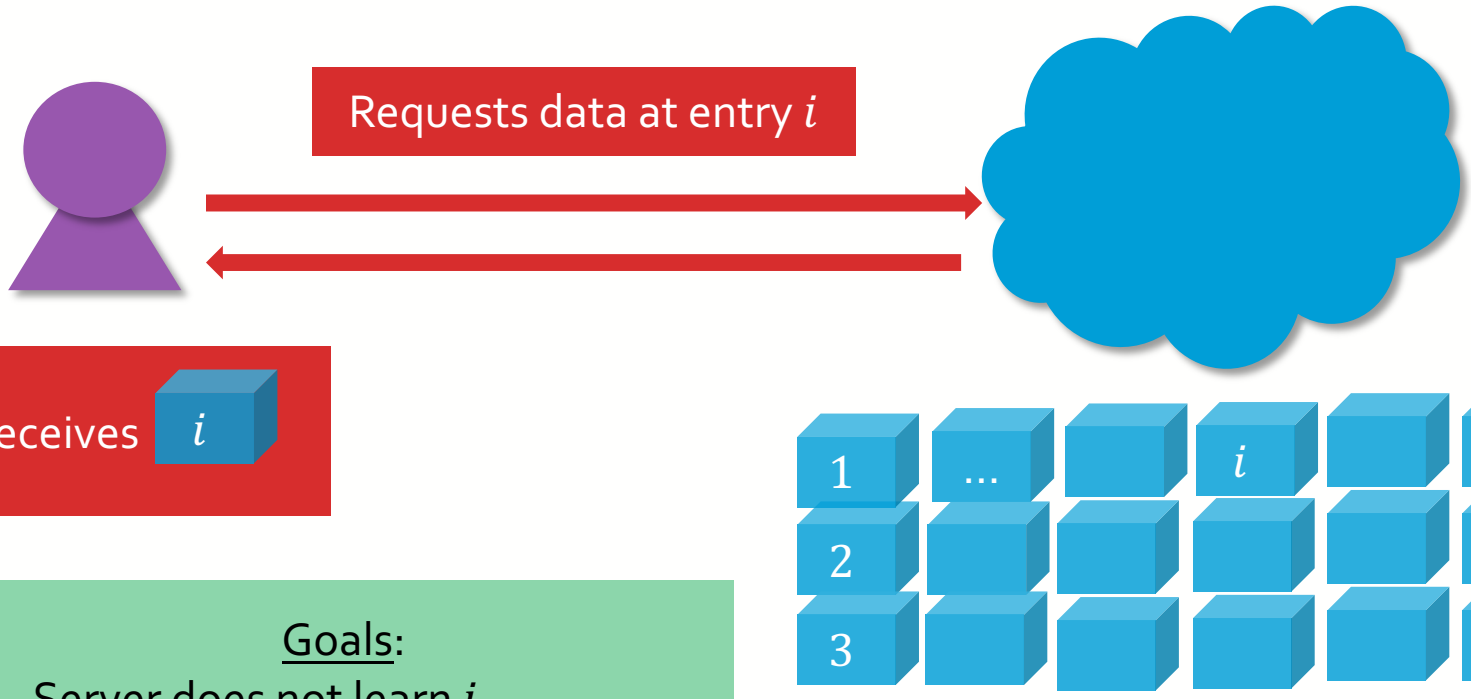
Private Information Retrieval (PIR)



Goals:

- Server does not learn i
- Communication cost is less than downloading whole database (N)

Private Information Retrieval (PIR)



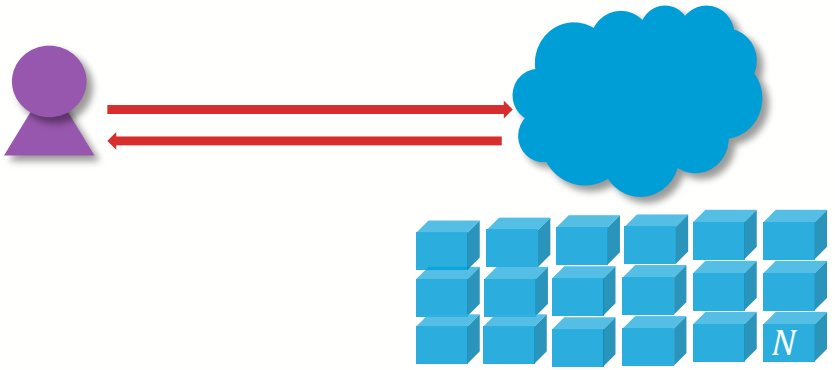
Goals:

- Server does not learn i
- Communication cost is less than downloading whole database (N)

PIR can be achieved from HE with data x encoding i and polynomial $f_{DB}(x)$ encoding function "retrieve data at location x "

Doubly-Efficient PIR (DEPIR)

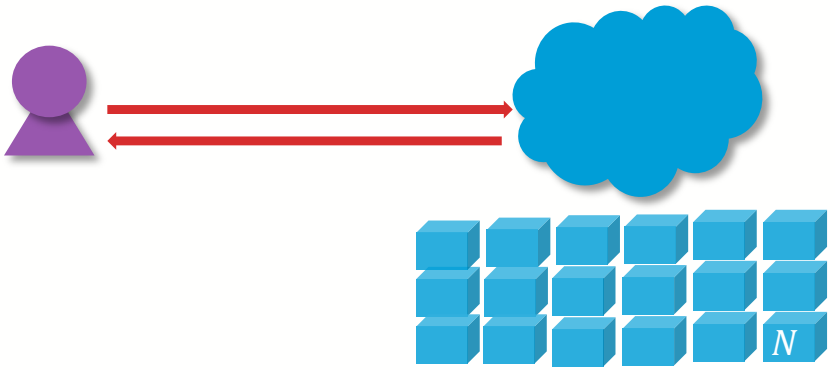
- Communication cost should be sublinear in N
- What about computational cost?



[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?

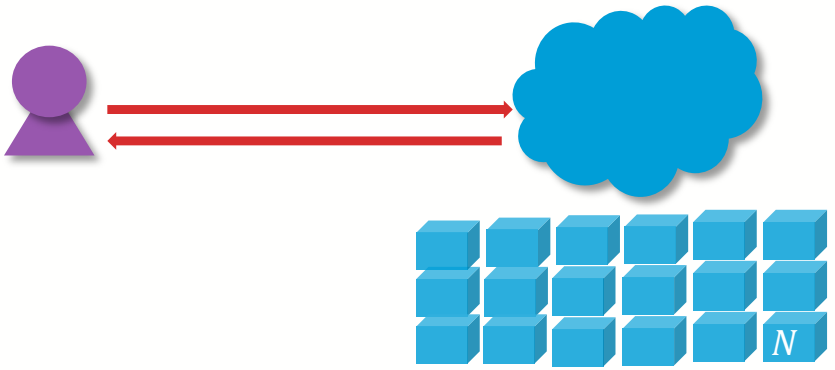


Preprocessing?

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

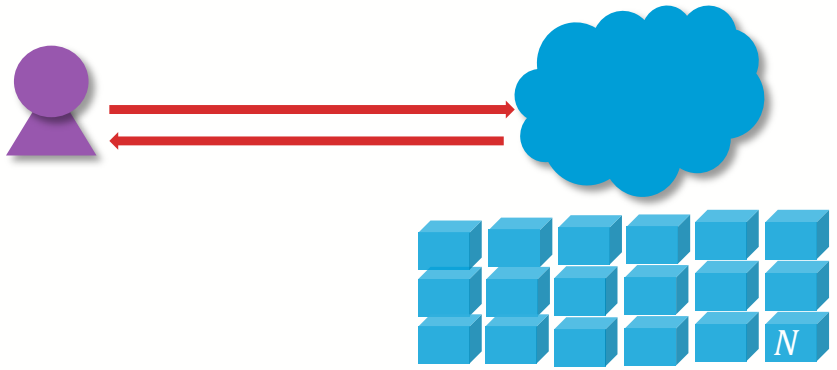
No

Computational cost must be $\Omega(N)$ [BIM00]

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

No

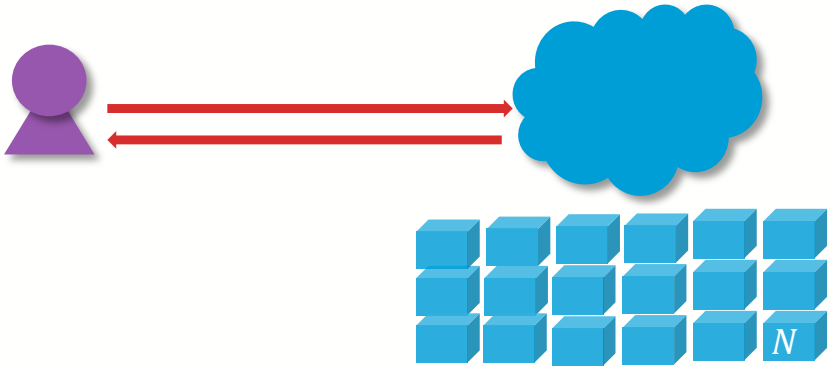
Yes

Computational cost must be $\Omega(N)$ [BIM00]

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

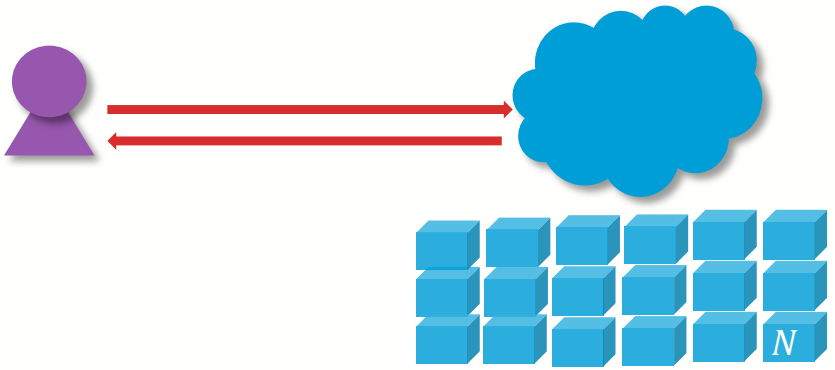
No → Computational cost must be $\Omega(N)$ [BIM00]

Yes → Client dependent: $\tilde{O}(N)$ cost per client

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

No → Computational cost must be $\Omega(N)$ [BIM00]

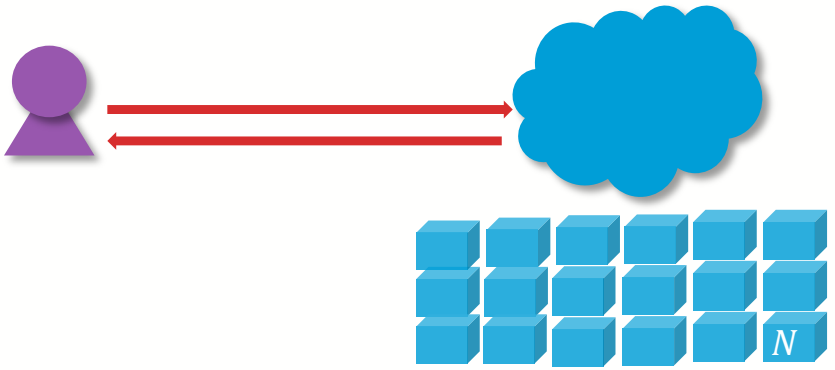
Yes → Client dependent: $\tilde{O}(N)$ cost per client

Yes → Client independent: one-time $\tilde{O}(N)$ cost

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

No

Yes

Computational cost must be $\Omega(N)$ [BIM00]

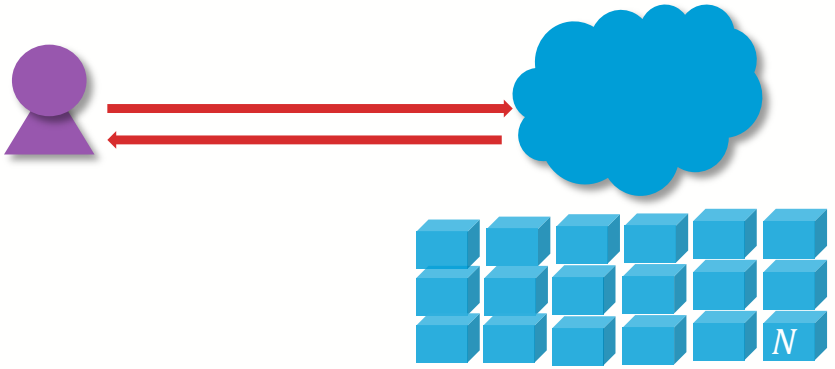
Client dependent: $\tilde{O}(N)$ cost per client

Client independent: one-time $\tilde{O}(N)$ cost

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Doubly-Efficient PIR (DEPIR)

- Communication cost should be sublinear in N
- What about computational cost?



Preprocessing?

No → Computational cost must be $\Omega(N)$ [BIM00]

Yes → Client dependent: $\tilde{O}(N)$ cost per client

Yes → Client independent: one-time $\tilde{O}(N)$ cost → DEPIR [LMW23]: Schemes in this setting with online cost sublinear in N

[BIM00] A. Beimel, Y. Ishai, T. Malkin. Reducing the Servers Computation in Private Information Retrieval: PIR with Preprocessing. CRYPTO 2000.
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

DEPIR construction of [LMW23]

ROYAL HOLLOWAY UNIVERSITY OF LONDON

[KU11, Theorem 2.1]
Let $f \in R[X_1, \dots, X_m]$ be a degree-d polynomial. Then we can build a datastructure that allows us to compute $f(x_1, \dots, x_m)$ in time poly$(d, m, \log \#R)$

[KU11] K. S. Kedlaya and C. Umans. Fast Polynomial Factorization and Modular Composition. SIAM J. Comput. 40.6 (2011)
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

DEPIR construction of [LMW23]

[KU11, Theorem 2.1]
Let $f \in R[X_1, \dots, X_m]$ be a degree-d polynomial. Then we can build a datastructure that allows us to compute $f(x_1, \dots, x_m)$ in time poly$(d, m, \log \#R)$

Main idea of [LMW23]:
Use [KU11] to efficiently compute f_{DB}!

[KU11] K. S. Kedlaya and C. Umans. Fast Polynomial Factorization and Modular Composition. SIAM J. Comput. 40.6 (2011)
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

DEPIR construction of [LMW23]

[KU11, Theorem 2.1]
Let $f \in R[X_1, \dots, X_m]$ be a degree-d polynomial. Then we can build a datastructure that allows us to compute $f(x_1, \dots, x_m)$ in time poly$(d, m, \log \#R)$

Main idea of [LMW23]:
Use [KU11] to efficiently compute f_{DB}!

Problem:
While f_{DB} is a polynomial, Eval$(f_{DB}, \cdot)$ may not be (e.g. due to modulus switching, relinearisation)

[KU11] K. S. Kedlaya and C. Umans. Fast Polynomial Factorization and Modular Composition. SIAM J. Comput. 40.6 (2011)
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

DEPIR construction of [LMW23]

[KU11, Theorem 2.1]
Let $f \in R[X_1, \dots, X_m]$ be a degree-d polynomial. Then we can build a datastructure that allows us to compute $f(x_1, \dots, x_m)$ in time poly$(d, m, \log \#R)$

Algebraic Somewhat Homomorphic Encryption (ASHE)

A somewhat homomorphic encryption scheme such that for polynomial f:

$$\text{Eval}(f, ct_1, \dots, ct_m) = f(ct_1, \dots, ct_m)$$

Main idea of [LMW23]:
Use [KU11] to efficiently compute f_{DB}!

Problem:
While f_{DB} is a polynomial, Eval(f_{DB} ,·) may not be (e.g. due to modulus switching, relinearisation)

[KU11] K. S. Kedlaya and C. Umans. Fast Polynomial Factorization and Modular Composition. SIAM J. Comput. 40.6 (2011)
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

DEPIR construction of [LMW23]

[KU11, Theorem 2.1]
Let $f \in R[X_1, \ldots, X_m]$ be a degree-d polynomial. Then we can build a datastructure that allows us to compute $f(x_1, \ldots, x_m)$ in time poly$(d, m, \log \#R)$

Algebraic Somewhat Homomorphic Encryption (ASHE)

A somewhat homomorphic encryption scheme such that for polynomial f:

$$\text{Eval}(f, ct_1, \ldots, ct_m) = f(ct_1, \ldots, ct_m)$$

Main idea of [LMW23]:
Use [KU11] to efficiently compute f_{DB}!

Problem:
While f_{DB} is a polynomial, Eval(f_{DB} ,·) may not be (e.g. due to modulus switching, relinearisation)

The ciphertext space must be a ring!

[KU11] K. S. Kedlaya and C. Umans. Fast Polynomial Factorization and Modular Composition. SIAM J. Comput. 40.6 (2011)
[LMW23] W. Lin, E. Mook, D. Wichs. Doubly Efficient Private Information Retrieval and Fully Homomorphic RAM Computation from Ring LWE. STOC 2023.

Our contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Performance of ASHE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem (informal)

A post-quantum ASHE scheme that can evaluate polynomials of degree d has ciphertext ring size $\Omega(2^d)$

Performance of ASHE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem (informal)
A post-quantum ASHE scheme that can evaluate polynomials of degree d has ciphertext ring size $\Omega(2^d)$

→ Lower bound on performance of post-quantum ASHE

Performance of ASHE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem (informal)
A post-quantum ASHE scheme that can evaluate polynomials of degree d has ciphertext ring size $\Omega(2^d)$

→ Lower bound on performance of post-quantum ASHE

Scheme	ASHE?	Ciphertext ring/space size
BGV, BFV	☒	$O(\text{poly}(d))$
BV	☑	$O(2^{d^2})$

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.
[BGV12] Z. Brakerski, C. Gentry, V. Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ITCS 2012.
[Bra12] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. CRYPTO 2012.
[FV12] J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. Eprint 2012/144.

Performance of ASHE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Theorem (informal)
A post-quantum ASHE scheme that can evaluate polynomials of degree d has ciphertext ring size $\Omega(2^d)$

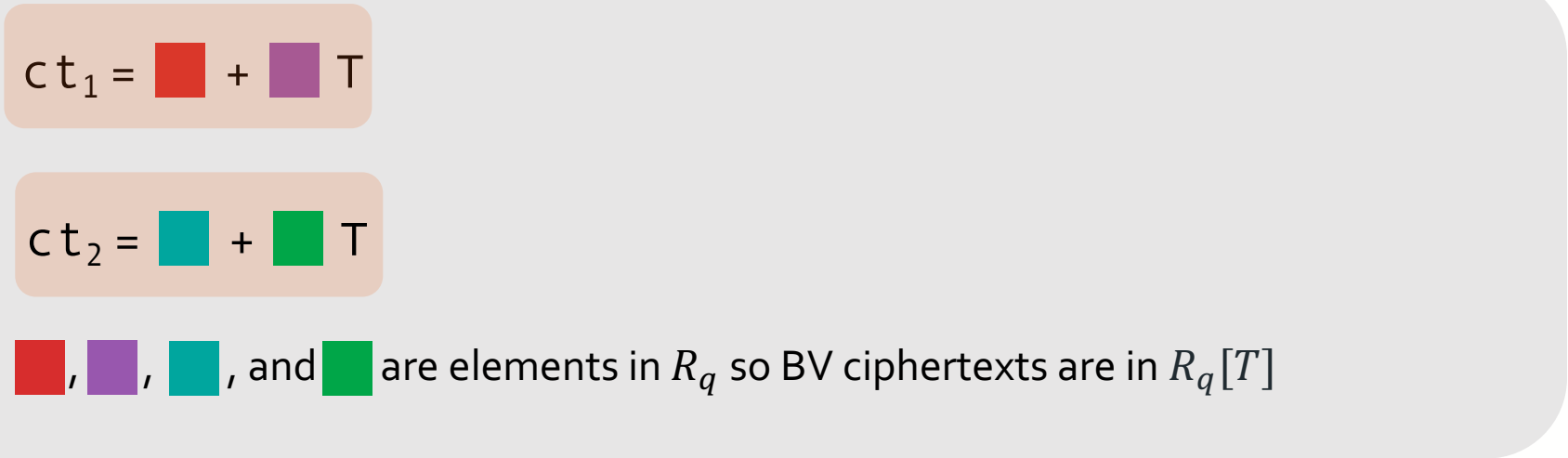
→ Lower bound on performance of post-quantum ASHE

Scheme	ASHE?	Ciphertext ring/space size
BGV, BFV	☒	$O(\text{poly}(d))$
BV	☑	$O(2^{d^2})$

→ Can we build ASHE with ciphertext ring size $O(2^d)$?

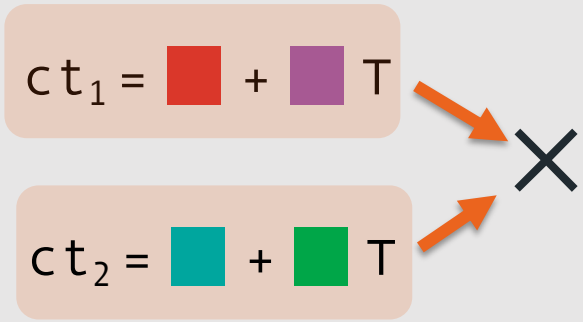
[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.
[BGV12] Z. Brakerski, C. Gentry, V. Vaikuntanathan. (Leveled) Fully Homomorphic Encryption without Bootstrapping. ITCS 2012.
[Bra12] Z. Brakerski. Fully Homomorphic Encryption without Modulus Switching from Classical GapSVP. CRYPTO 2012.
[FV12] J. Fan and F. Vercauteren. Somewhat Practical Fully Homomorphic Encryption. Eprint 2012/144.

Modified BV



[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

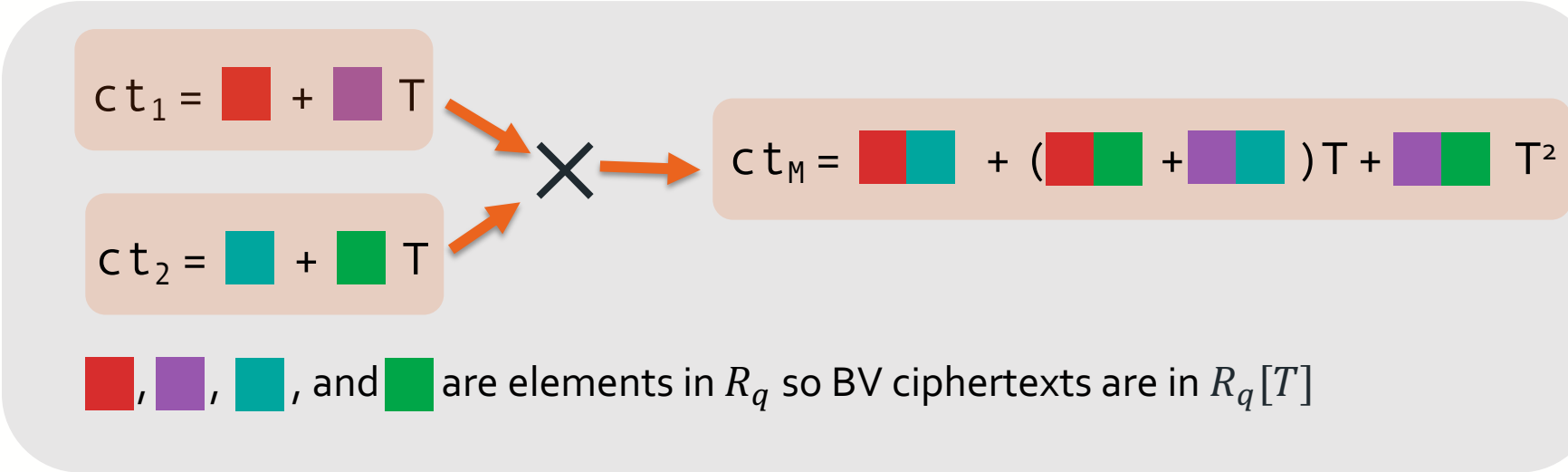
Modified BV



, , , and are elements in R_q so BV ciphertexts are in $R_q[T]$

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

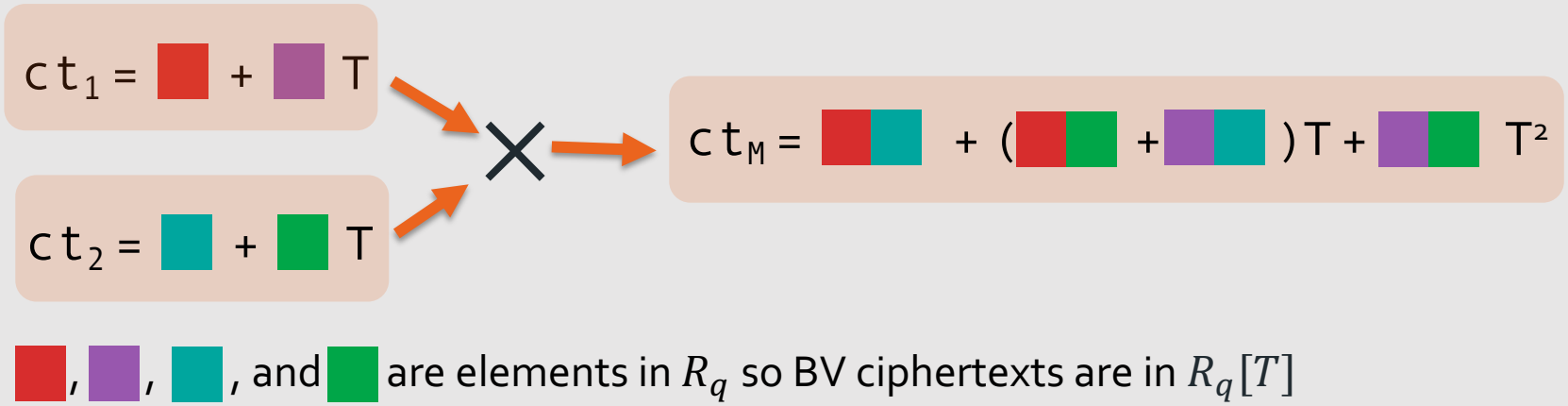
Modified BV



[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

Idea: Use double CRT to work over $\mathbb{F}_p[T]$ instead of $R_q[T]$



[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

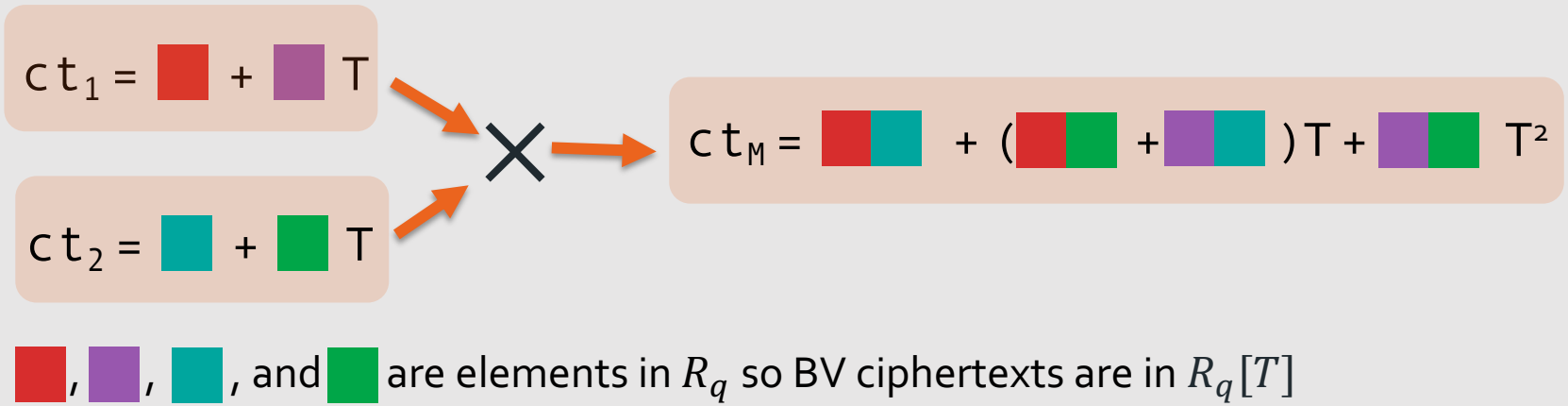
Modified BV

Idea: Decompose the polynomial f being evaluated as

$$f(b_1 + a_1 T, \ldots, b_m + a_m T) = \sum_i T^i f_i(a_1, \ldots, a_m, b_1, \ldots, b_m)$$

to evaluate $2m$-variate polynomials over $\mathbb{F}_p$

Idea: Use double CRT to work over $\mathbb{F}_p[T]$ instead of $R_q[T]$



, , , and are elements in R_q so BV ciphertexts are in $R_q[T]$

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

$$f(b_1 + a_1 T, \dots, b_m + a_m T) = \sum_i T^i f_i(a_1, \dots, a_m, b_1, \dots, b_m)$$

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

$$f(b_1 + a_1 T, \dots, b_m + a_m T) = \sum_i T^i f_i(a_1, \dots, a_m, b_1, \dots, b_m)$$

Main idea: fix $b_i \in \{0,1\}$ and do DEPIR precomputation once for each $(b_1, \dots, b_m) \in \{0,1\}^m$ on the polynomial $f_{i,b_1,\dots,b_m}(a_1, \dots, a_m)$

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

$$f(b_1 + a_1 T, \dots, b_m + a_m T) = \sum_i T^i f_i(a_1, \dots, a_m, b_1, \dots, b_m)$$

Main idea: fix $b_i \in \{0,1\}$ and do DEPIR precomputation once for each $(b_1, \dots, b_m) \in \{0,1\}^m$ on the polynomial $f_{i,b_1,\dots,b_m}(a_1, \dots, a_m)$

Having m instead of $2m$ variables reduces storage

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

$$f(b_1 + a_1 T, \dots, b_m + a_m T) = \sum_i T^i f_i(a_1, \dots, a_m, b_1, \dots, b_m)$$

Main idea: fix $b_i \in \{0,1\}$ and do DEPIR precomputation once for each $(b_1, \dots, b_m) \in \{0,1\}^m$ on the polynomial $f_{i,b_1,\dots,b_m}(a_1, \dots, a_m)$

Having m instead of $2m$ variables reduces storage

ct =  +  T

( , ) is a RLWE sample

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

Modified BV

$$f(b_1 + a_1 T, \dots, b_m + a_m T) = \sum_i T^i f_i(a_1, \dots, a_m, b_1, \dots, b_m)$$

Main idea: fix $b_i \in \{0,1\}$ and do DEPIR precomputation once for each $(b_1, \dots, b_m) \in \{0,1\}^m$ on the polynomial $f_{i,b_1,\dots,b_m}(a_1, \dots, a_m)$

Having m instead of $2m$ variables reduces storage

Fixing $b_i \in \{0,1\}$ means modifying the underlying RLWE assumption to one where the the "b" part has CRT components in $\{0,1\}$

c t = + T

(,) is a RLWE sample

[BV11] Z. Brakerski,V. Vaikuntanathan. Fully Homomorphic Encryption from Ring-LWE and Security for Key Dependent Messages. CRYPTO 2011.

$\{0,1\}$-CRT-RLWE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Definition ($\{0,1\}$-CRT set)

Define S as the set of elements in R_q such that $S := \iota^{-1}(\{0,1\}^{nr})$ where ι is the double-CRT isomorphism and r is the number of divisors of q.

$\{0,1\}$-CRT-RLWE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Definition ($\{0,1\}$-CRT set)

Define S as the set of elements in R_q such that $S := \iota^{-1}(\{0,1\}^{nr})$ where ι is the double-CRT isomorphism and r is the number of divisors of q.

Definition (Decision $\{0,1\}$-CRT-RLWE)

Let $s \in R_q$ be secret. Distinguish samples (a_i, b_i) from uniform, where $b_i \in S$ and $a_i = s^{-1}(b_i - e_i)$ for e_i chosen from some small error distribution.

$\{0,1\}$-CRT-RLWE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Definition ($\{0,1\}$-CRT set)

Define S as the set of elements in R_q such that $S := \iota^{-1}(\{0,1\}^{nr})$ where ι is the double-CRT isomorphism and r is the number of divisors of q.

Definition (Decision $\{0,1\}$-CRT-RLWE)

Let $s \in R_q$ be secret. Distinguish samples (a_i, b_i) from uniform, where $b_i \in S$ and $a_i = s^{-1}(b_i - e_i)$ for e_i chosen from some small error distribution.

Theorem (informal)

Let q satisfy some technical constraints. If standard RLWE with preprocessing on R_q is hard, then $\{0,1\}$-CRT-RLWE with preprocessing on R_q is also hard.

$\{0,1\}$-CRT-RLWE

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Definition ($\{0,1\}$-CRT set)

Define S as the set of elements in R_q such that $S := \iota^{-1}(\{0,1\}^{nr})$ where ι is the double-CRT isomorphism and r is the number of divisors of q.

Definition (Decision $\{0,1\}$-CRT-RLWE)

Let $s \in R_q$ be secret. Distinguish samples (a_i, b_i) from uniform, where $b_i \in S$ and $a_i = s^{-1}(b_i - e_i)$ for e_i chosen from some small error distribution.

Theorem (informal)

Let q satisfy some technical constraints. If standard RLWE with preprocessing on R_q is hard, then $\{0,1\}$-CRT-RLWE with preprocessing on R_q is also hard.

The adversary is allowed to run a preprocessing phase with only R and q as input before querying the RLWE oracle

Performance compared to [OPPW24]

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Reduction in read queries:

- $8\times$ for parameters we can run
- $23\times$ for larger parameters

[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Performance compared to [OPPW24]

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Reduction in read queries:
- $8\times$ for parameters we can run
- $23\times$ for larger parameters

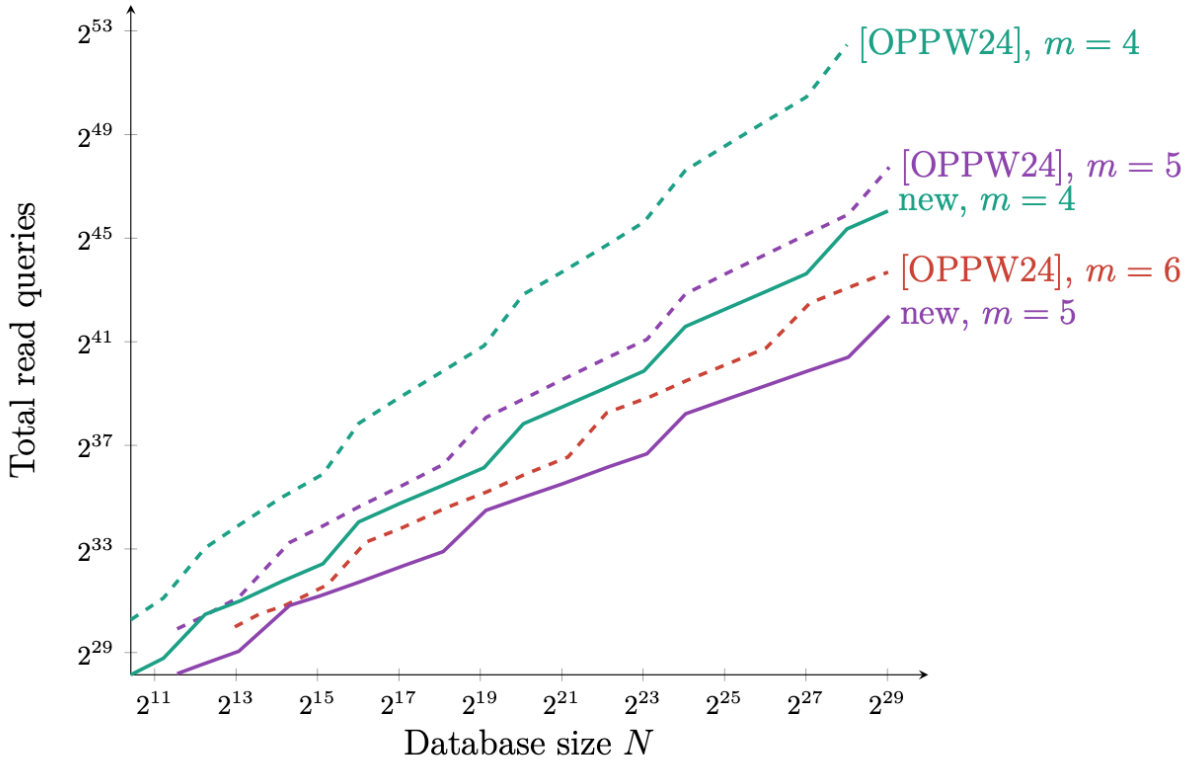
Speedup of more than $4\times$

[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Performance compared to [OPPW24]

Reduction in read queries:
- 8× for parameters we can run
- 23× for larger parameters

Speedup of more than 4×

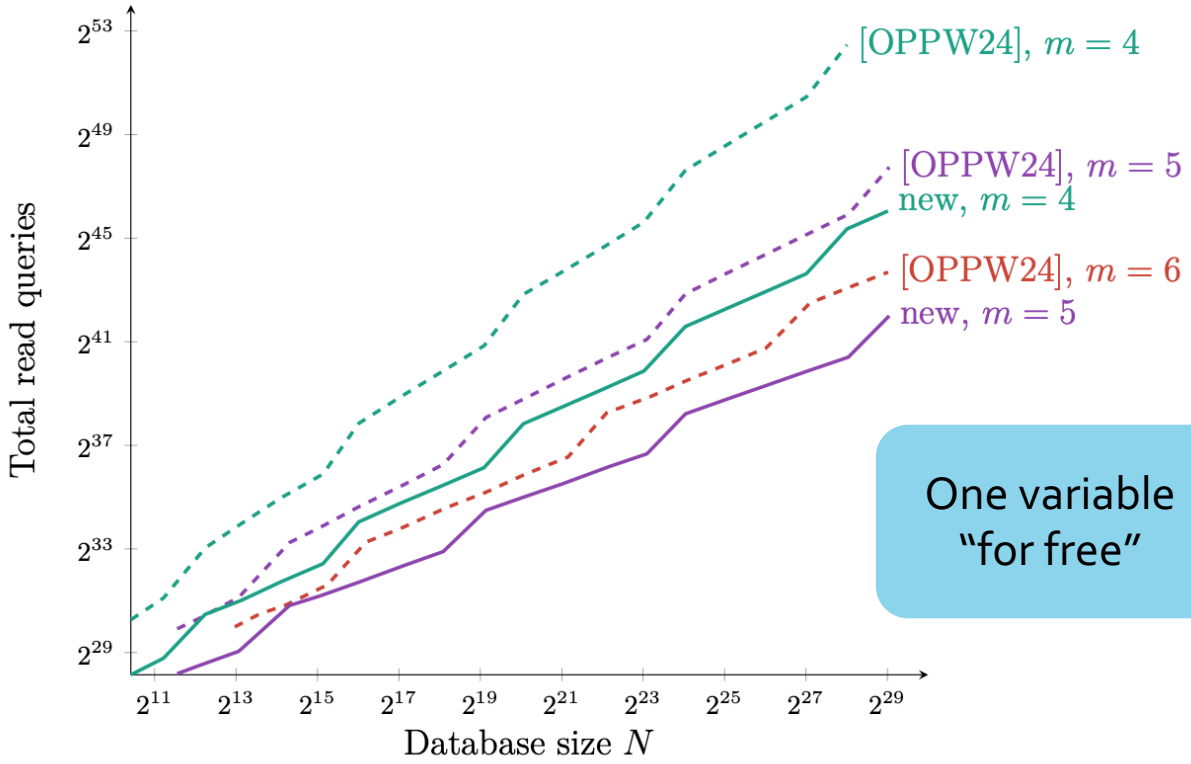


[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Performance compared to [OPPW24]

Reduction in read queries:
- 8× for parameters we can run
- 23× for larger parameters

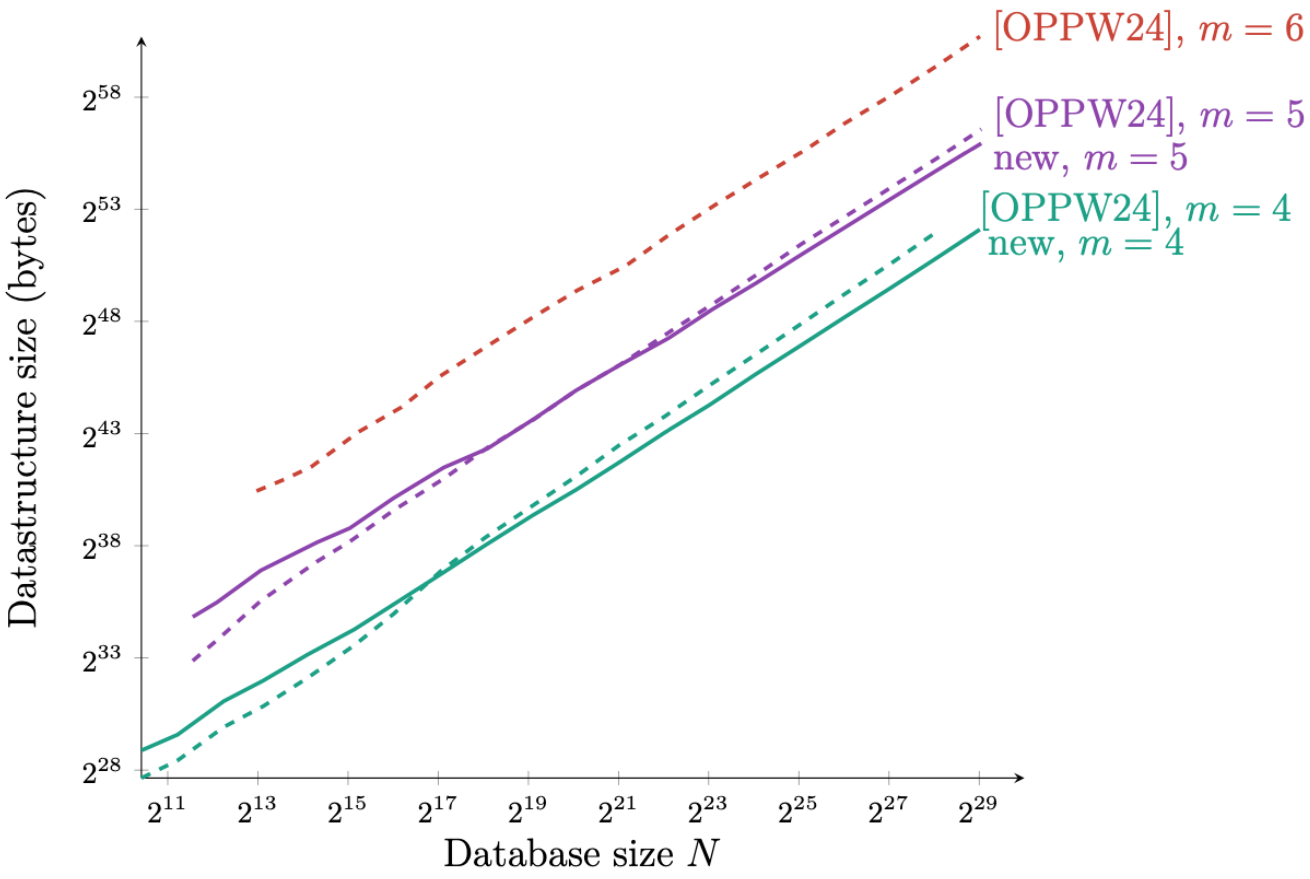
Speedup of more than 4×



One variable "for free"

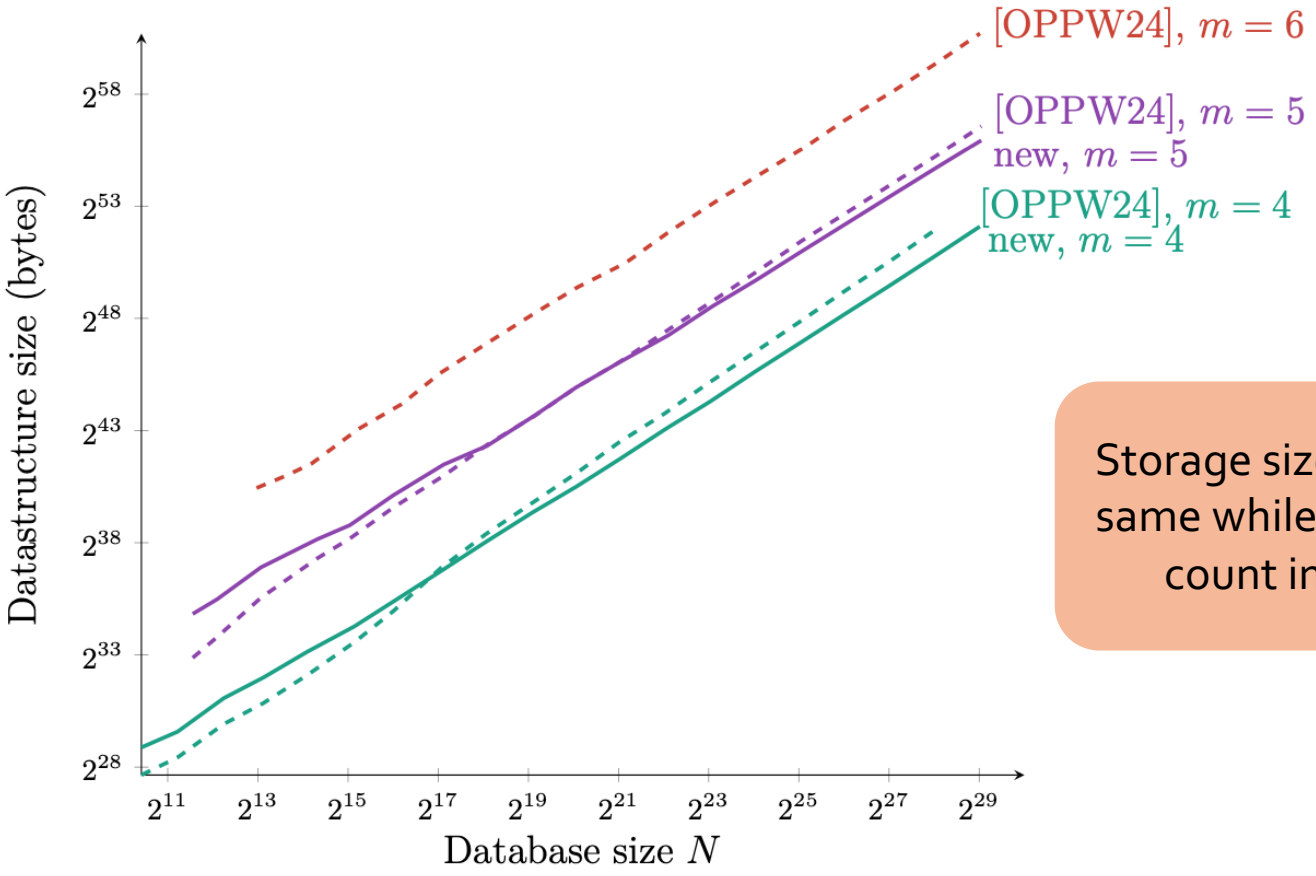
[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Performance compared to [OPPW24]



[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Performance compared to [OPPW24]



Storage size about the same while read query count improves

[OPPW24] H. Okada, R. Player, S. Pohmann, C. Weinert. Towards Practical Doubly-Efficient Private Information Retrieval. Financial Cryptography 2024.

Conclusion

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Modified BV scheme based on $\{0,1\}$-CRT-RLWE

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Modified BV scheme based on $\{0,1\}$-CRT-RLWE

Additional improvement to polynomial evaluation datastructure

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Modified BV scheme based on $\{0,1\}$-CRT-RLWE

Additional improvement to polynomial evaluation datastructure

Improved DEPIR implementation

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Modified BV scheme based on $\{0,1\}$-CRT-RLWE

Additional improvement to polynomial evaluation datastructure

Improved DEPIR implementation

Reduction from RLWE to certain reduced entropy variants of RLWE, including $\{0,1\}$-CRT-RLWE

Summary of contributions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Lower bound on performance of post-quantum ASHE

Modified BV scheme based on $\{0,1\}$-CRT-RLWE

Additional improvement to polynomial evaluation datastructure

Improved DEPIR implementation

Reduction from RLWE to certain reduced entropy variants of RLWE, including $\{0,1\}$-CRT-RLWE

Preliminary cryptanalysis of $\{0,1\}$-CRT-RLWE

Open questions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Does there exist an ASHE scheme that can evaluate circuits of depth d with ciphertext ring size $O(2^d)$?

Open questions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Does there exist an ASHE scheme that can evaluate circuits of depth d with ciphertext ring size $O(2^d)$?

Are there other relaxations of ASHE that are sufficient to construct DEPIR?

Open questions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Does there exist an ASHE scheme that can evaluate circuits of depth d with ciphertext ring size $O(2^d)$?

Are there other relaxations of ASHE that are sufficient to construct DEPIR?

Are there other approaches for more efficient DEPIR?

Open questions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Does there exist an ASHE scheme that can evaluate circuits of depth d with ciphertext ring size $O(2^d)$?

Are there other relaxations of ASHE that are sufficient to construct DEPIR?

Are there other approaches for more efficient DEPIR?

Is $\{0,1\}$-CRT-RLWE concretely as hard as RLWE?

Open questions

ROYAL HOLLOWAY UNIVERSITY OF LONDON

Does there exist an ASHE scheme that can evaluate circuits of depth d with ciphertext ring size $O(2^d)$?

Are there other relaxations of ASHE that are sufficient to construct DEPIR?

Are there other approaches for more efficient DEPIR?

Is $\{0,1\}$-CRT-RLWE concretely as hard as RLWE?

Are our reduced entropy RLWE variants useful for other applications?

Thank you!
Any questions?

Full version on eprint: 2024/1307
Implementation: github.com/FeanorTheElf/ashe-depir

rachel.player@rhul.ac.uk
https://rachelplayer.github.io

ROYAL HOLLOWAY UNIVERSITY OF LONDON