AN ANALYSIS OF FV PARAMETERS IMPACT TOWARDS ITS HARDWARE ACCELERATION

Joël Cathébras, Alexandre Carbon, Renaud Sirdey, Nicolas Ventroux

Journées Codage & Cryptographie 2017 | 25 Avril 2017 | La Bresse

INTRODUCTION

- **Homomorphic encryption:**
  Handling private data on untrusted environment

- **Decryption function is an homomorphism:**

c_1, c_2 two ciphertexts such that
$c_1 = \mathrm{Enc}(m_1)$ and $c_2 = \mathrm{Enc}(m_2)$

$$\Rightarrow \begin{cases} \mathrm{Dec}(c_1) \circ \mathrm{Dec}(c_2) = \mathrm{Dec}(c_1 \odot c_2) \\ m_1 \circ m_2 \Leftrightarrow c_1 \odot c_2 \end{cases}$$

- **User requirements:**
  - Security level
  - Application complexity (multiplicative depth)

⇒ **Impact**

- **Main issues:**
  - Noise management
  - Data size overhead
  - Primitive performances

STATE OF THE ART (1)
HOMOMORPHIC SCHEMES

First generation

- **2009: Gentry bootstrapping**
  Fully Homomorphic Encryption scheme

Impractical

Second generation

- **2011: BGV scheme**
  Modulus-switching noise management
- **2012: FV scheme**
  Scale invariant noise management

Small applications already!

Third generation

- **2013: GSW scheme**
  Simplified FHE construction
- **2016: Chillotti et al.**
  Bootstrapping in less than 0.1s

Promising

STATE OF THE ART (1)
HOMOMORPHIC SCHEMES

First generation	• **2009: Gentry bootstrapping** Fully Homomorphic Encryption scheme	**Impractical**
Second generation	• **2011: BGV scheme** Modulus-switching noise management • **2012: FV scheme** Scale invariant noise management	**Small applications already!**
Third generation	• **2013: GSW scheme** Simplified FHE construction • **2016: Chillotti et al.** Bootstrapping in less than 0.1s	**Promising**

Practically removal of the FHE encryption bottleneck

2015: Stream-cipher based transciphering

STATE OF THE ART (1)
HOMOMORPHIC SCHEMES

First generation

- **2009: Gentry bootstrapping**
  Fully Homomorphic Encryption scheme

Impractical

Second generation

- **2011: BGV scheme**
  Modulus-switching noise management
- **2012: FV scheme**
  Scale invariant noise management

Small applications already!

Third generation

- **2013: GSW scheme**
  Simplified FHE construction
- **2016: Chillotti et al.**
  Bootstrapping in less than 0.1s

Promising

Practically removal of the FHE encryption bottleneck
2015: Stream-cipher based transciphering

Hardware optimizations could leverage practicability of homomorphic encryption

STATE OF THE ART (2)

PARAMETERS

- **Implementation level parameters:**
  - Cyclotomic polynomial degree N
  - Ciphertext modulus size $T_q = \log_2 q$

STATE OF THE ART (2)

PARAMETERS

- **Parameters derivation for FV like scheme:**
  - Lattice problem dimensioning
  - Security requirement λ
  - Multiplicative depth requirement L

Derivation

User requirements

- **Implementation level parameters:**
  - Cyclotomic polynomial degree N
  - Ciphertext modulus size $T_q = \log_2 q$

STATE OF THE ART (2)

PARAMETERS

- **Parameters derivation for FV like scheme:**
  - Lattice problem dimensioning
  - Security requirement λ
  - Multiplicative depth requirement L

↓ **Derivation**

User requirements

- **Implementation level parameters:**
  - Cyclotomic polynomial degree N
  - Ciphertext modulus size $T_q = \log_2 q$

↓ **Impact**

- **Hardware optimization opportunities:**
  - RNS arithmetic
  - NTT-based polynomial multiplication

STATE OF THE ART (2)
PARAMETERS

- **Parameters derivation for FV like scheme:**
  - Lattice problem dimensioning
  - Security requirement λ
  - Multiplicative depth requirement L

Derivation

- **Implementation level parameters:**
  - Cyclotomic polynomial degree N
  - Ciphertext modulus size $T_q = \log_2 q$

Impact

- **Hardware optimization opportunities:**
  - RNS arithmetic
  - NTT-based polynomial multiplication

User requirements

Contribution: hardware optimization viewpoint

OVERVIEW

Introduction

Context of this work

Optimization analysis for FV like schemes

Parameter tradeoff analysis

Conclusion and perspectives

STREAM CIPHER BASED TRANSCIPHERING

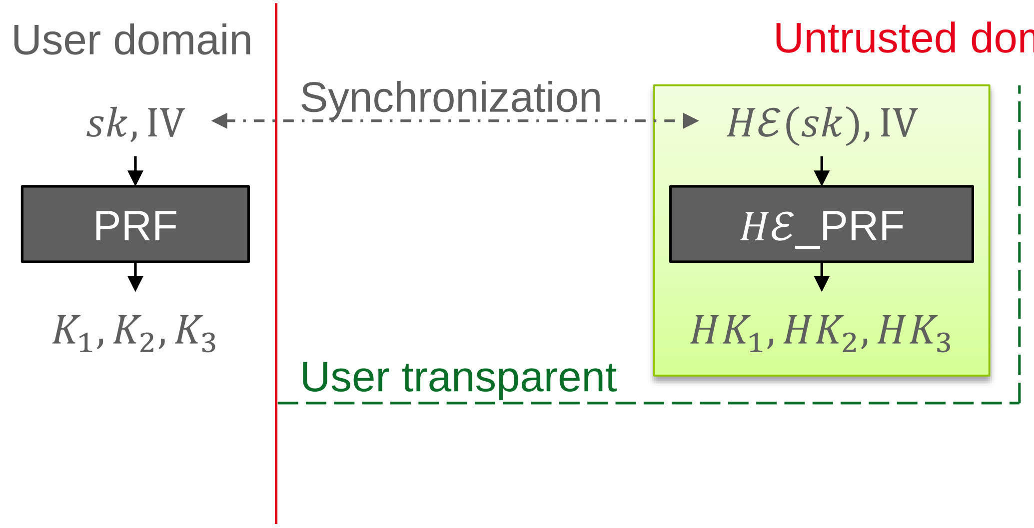
Transciphering: avoid upward communication overhead

User domain

Untrusted domain

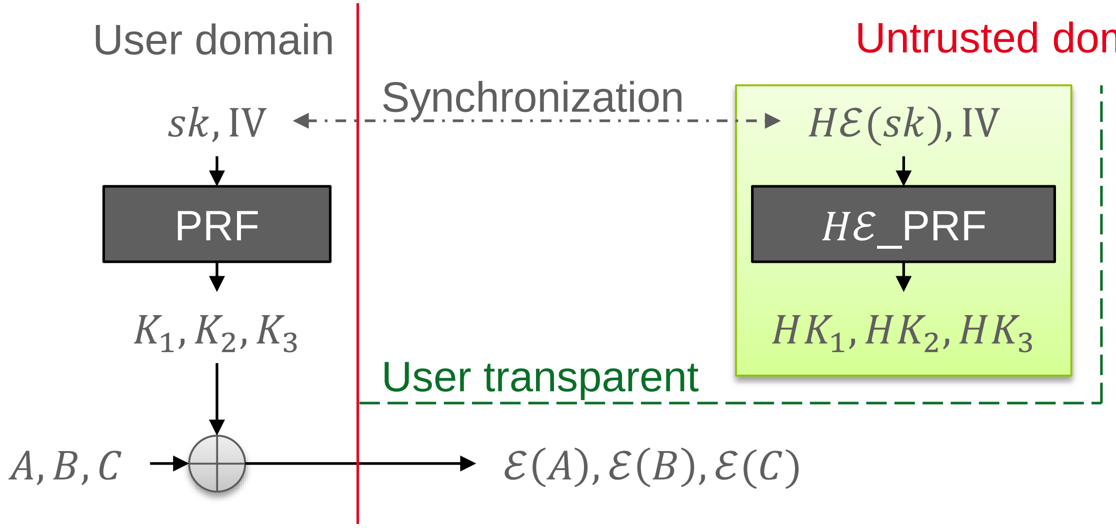
STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead



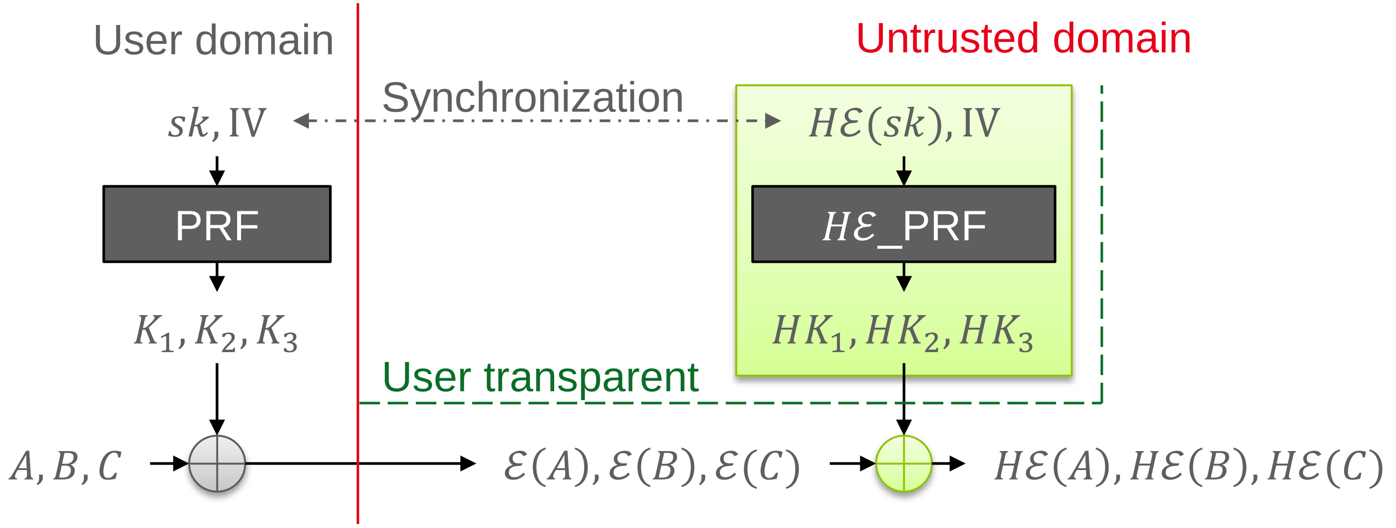
STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead



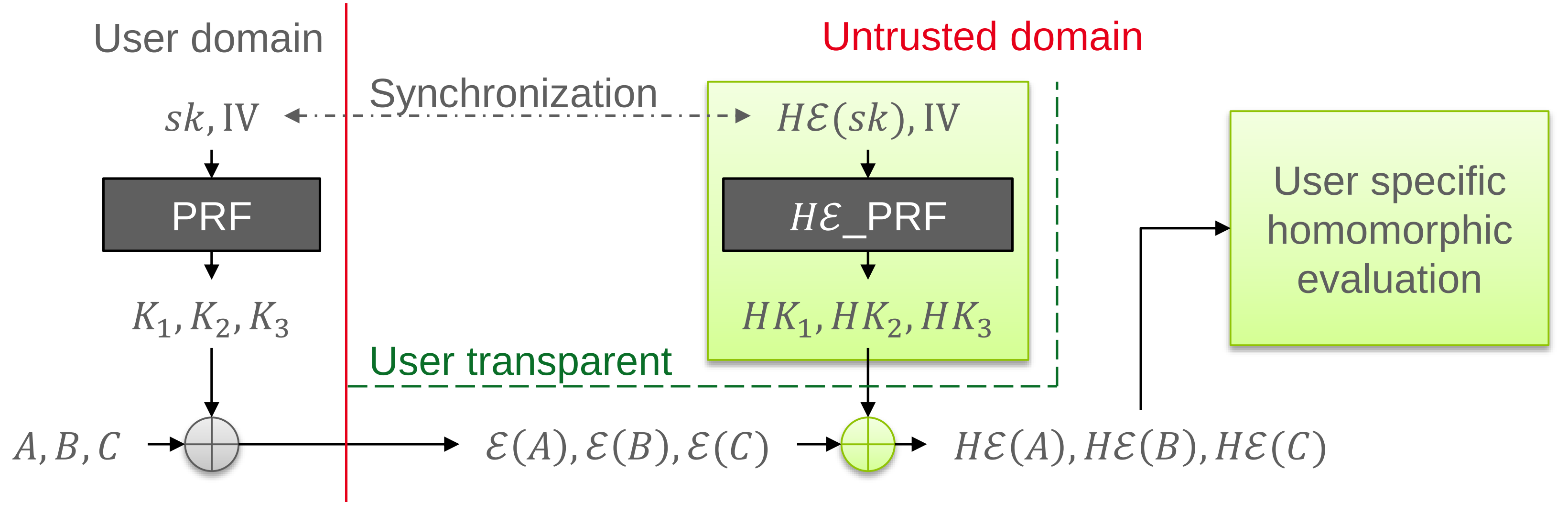
STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead



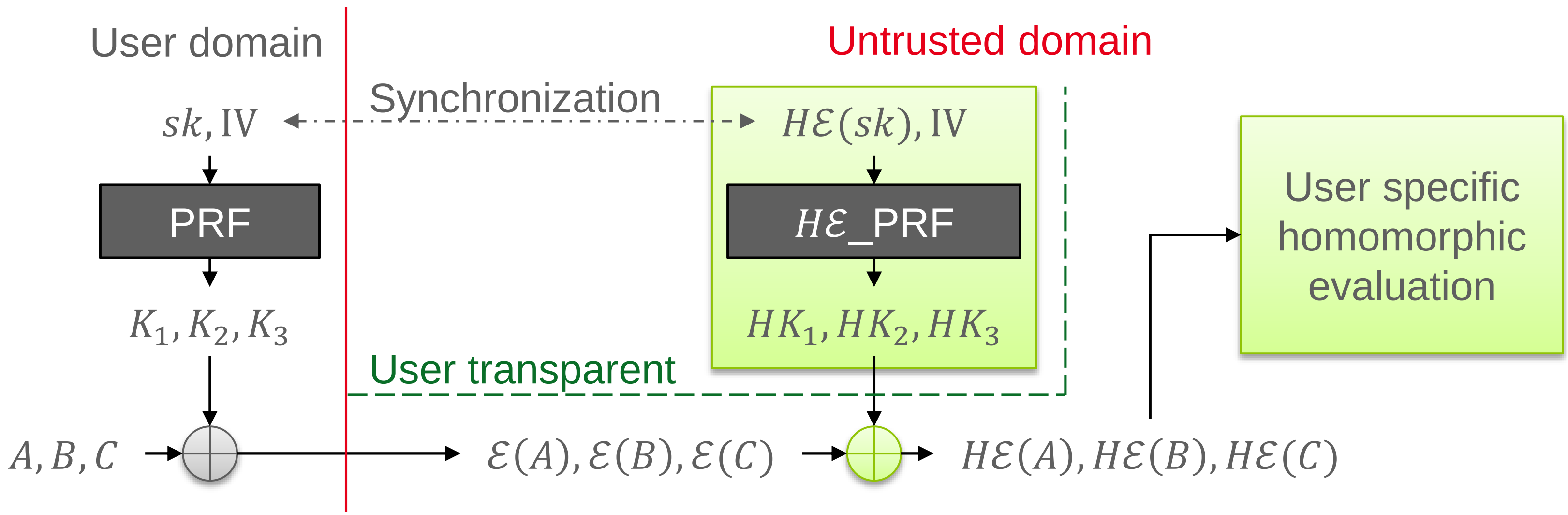
STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead



STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead

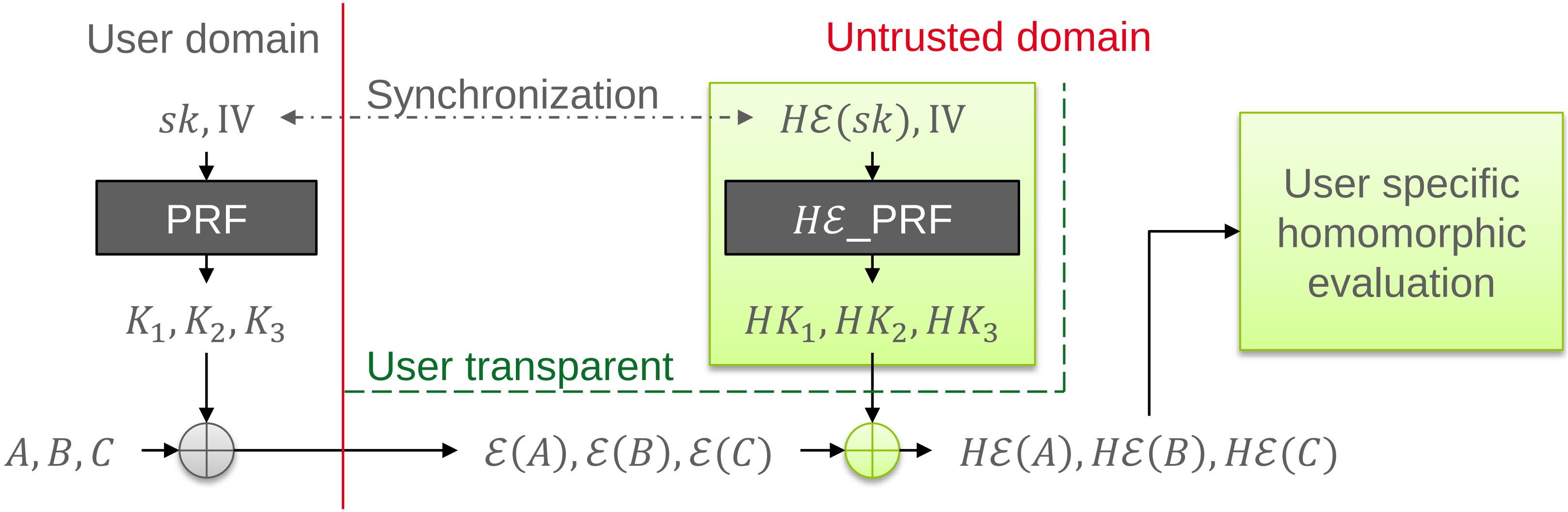


Improving homomorphic evaluation

Leverage homomorphic keystream generation

STREAM CIPHER BASED TRANSCIPHERING

Transciphering: avoid upward communication overhead



Improving homomorphic evaluation

⇩

Leverage homomorphic keystream generation

Impact on parameters:

- Consistent security between HE and PRF
- Constant multiplicative depth penalty

STREAM CIPHER HOMOMORPHIC EVALUATION

- **FV homomorphic evaluation of Trivium* (**eSTREAM portfolio**):**

* ISO/IEC 29192-3:2012

STREAM CIPHER HOMOMORPHIC EVALUATION

- **FV homomorphic evaluation of Trivium* (**eSTREAM portfolio**):**

HE Primitives	Estimated cycles	Estimated %
HE Trivium	$\mathbf{13,33 \times 10^{12}}$	$\mathbf{100}$ %
CtxtMult	$\mathbf{13,27 \times 10^{12}}$	$\mathbf{99,5}$ %
- Relinearise	$8{,}38 \times 10^{12}$	$62{,}8$ %
- Multiply	$4{,}09 \times 10^{12}$	$30{,}6$ %
- Others	$0{,}81 \times 10^{12}$	$6{,}1$ %
CtxtAdd	$\mathbf{0,05 \times 10^{12}}$	$\mathbf{0,4}$ %
Others	$\mathbf{0,01 \times 10^{12}}$	$\mathbf{0,1}$ %

FV implementation from Canteaut et al. based on FLINT and GMP

FV instance:

- Security $\lambda = 80$
- Multiplicative depth $L = 19$
- Polynomial degree $N = 4096$
- Ciphertext modulus size $T_q = 2658$-bits

Algorithm	λ	FV		
		#ANDs	#XORs	keystream
Trivium-12	80	3237	15019	57

Outputs:

- 57 keystream elements per IV
- Useful multiplicative depth: 7

* ISO/IEC 29192-3:2012

STREAM CIPHER HOMOMORPHIC EVALUATION

- **FV homomorphic evaluation of Trivium* (**eSTREAM portfolio**):**

HE Primitives	Estimated cycles	Estimated %
HE Trivium	$\mathbf{13,33 \times 10^{12}}$	$\mathbf{100\ \%}$
CtxtMult	$\mathbf{13,27 \times 10^{12}}$	$\mathbf{99,5\ \%}$
- Relinearise	$8{,}38 \times 10^{12}$	$62{,}8\ \%$
- Multiply	$4{,}09 \times 10^{12}$	$30{,}6\ \%$
- Others	$0{,}81 \times 10^{12}$	$6{,}1\ \%$
CtxtAdd	$\mathbf{0,05 \times 10^{12}}$	$\mathbf{0,4\ \%}$
Others	$\mathbf{0,01 \times 10^{12}}$	$\mathbf{0,1\ \%}$

FV implementation from Canteaut et al. based on FLINT and GMP

FV instance:

- Security $\lambda = 80$
- Multiplicative depth $L = 19$
- Polynomial degree $N = 4096$
- Ciphertext modulus size $T_q = 2658$-bits

Algorithm	λ	FV		
		#ANDs	**#XORs**	**keystream**
Trivium-12	80	3237	15019	57

Outputs:

- 57 keystream elements per IV
- Useful multiplicative depth: 7

* ISO/IEC 29192-3:2012

STREAM CIPHER HOMOMORPHIC EVALUATION

- **FV homomorphic evaluation of Trivium* (**eSTREAM portfolio**):**

HE Primitives	Estimated cycles	Estimated %
HE Trivium	$\mathbf{13,33 \times 10^{12}}$	$\mathbf{100\ \%}$
CtxtMult	$\mathbf{13,27 \times 10^{12}}$	$\mathbf{99,5\ \%}$
- Relinearise	$8{,}38 \times 10^{12}$	$62{,}8\ \%$
- Multiply	$4{,}09 \times 10^{12}$	$30{,}6\ \%$
- Others	$0{,}81 \times 10^{12}$	$6{,}1\ \%$
CtxtAdd	$\mathbf{0,05 \times 10^{12}}$	$\mathbf{0,4\ \%}$
Others	$\mathbf{0,01 \times 10^{12}}$	$\mathbf{0,1\ \%}$

FV implementation from Canteaut et al. based on FLINT and GMP

FV instance:

- Security $\lambda = 80$
- Multiplicative depth $L = 19$
- Polynomial degree $N = 4096$
- Ciphertext modulus size $T_q = 2658$-bits

Algorithm	λ	FV		
		#ANDs	#XORs	keystream
Trivium-12	80	3237	15019	57

Outputs:

- 57 keystream elements per IV
- Useful multiplicative depth: 7

- **Underlying complexity:**
  - ~20%: Multi-precision arithmetic under the direct influence of T_q
  - ~75%: Polynomial multiplication under the direct influence of N

* ISO/IEC 29192-3:2012

FV PARAMETERS

- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**

  - Security level: λ
  - Multiplicative depth: L
  - Plaintext space $(t = 2)$
  - Distinguishing attack
    $([\mathrm{LP'11}]\ \varepsilon = 2^{-64} \Rightarrow\ \alpha = 3{,}758)$

  Derivation

  - Cyclotomic polynomial degree: N
    (secret Hamming weight $h = 63$)
  - Coefficient sizes: $T_q = \log_2 q$
    (parameter σ of the error distribution χ)

FV PARAMETERS

- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**

  - Security level: λ
  - Multiplicative depth: L
  - Plaintext space ($t = 2$)
  - Distinguishing attack ($[\mathrm{LP}'11]\ \varepsilon = 2^{-64} \Rightarrow\ \alpha = 3{,}758$)

Derivation

  - Cyclotomic polynomial degree: N (secret Hamming weight $h = 63$)
  - Coefficient sizes: $T_q = \log_2 q$ (parameter σ of the error distribution χ)

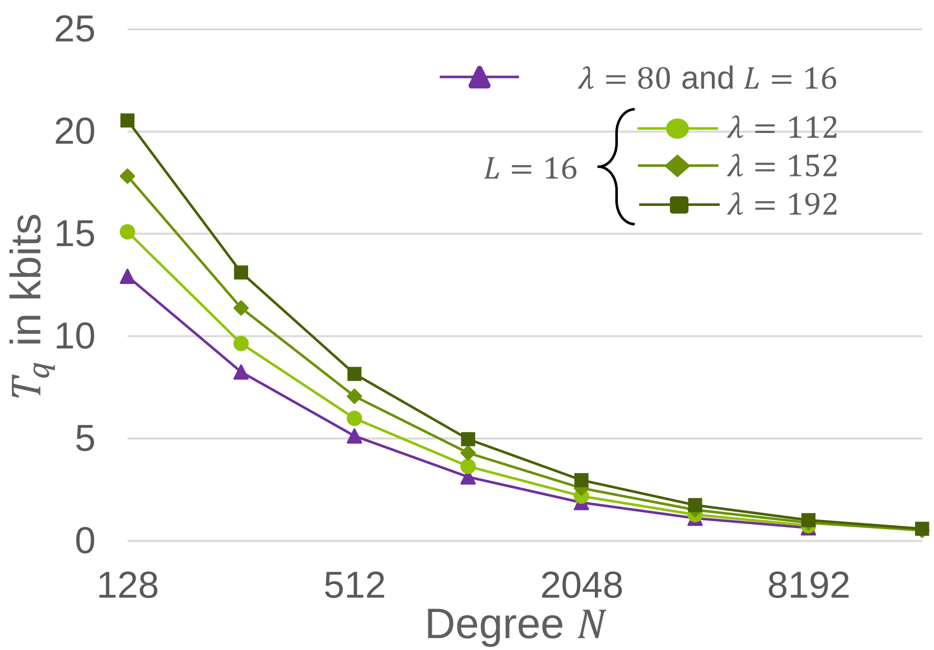
FV PARAMETERS

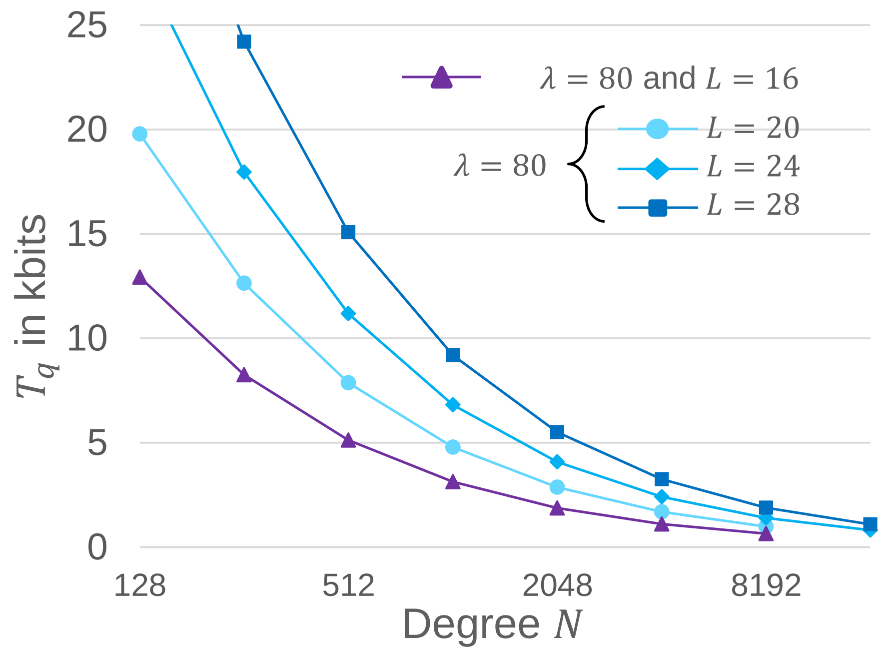
- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**
    - Security level: λ
    - Multiplicative depth: L
    - Plaintext space $(t = 2)$
    - Distinguishing attack ([LP′11] $\varepsilon = 2^{-64} \Rightarrow \alpha = 3{,}758$)

Derivation

- Cyclotomic polynomial degree: N (secret Hamming weight $h = 63$)
- Coefficient sizes: $T_q = \log_2 q$ (parameter σ of the error distribution χ)

- **Relation $T_q(N)$ for fixed (λ, L):**





OVERVIEW

Introduction

Context of this work

Optimization analysis for FV like schemes

Parameter tradeoff analysis

Conclusion and perspectives

HANDLING LARGE COEFFICIENT SIZES

CHINESE REMAINDER THEOREM – RNS ARITHMETIC

- **Ciphertexts are pairs of polynomials:**
  - Degree is fixed by the parameter N
  - Coefficients are integers modulo q (T_q-bits size)

HANDLING LARGE COEFFICIENT SIZES

CHINESE REMAINDER THEOREM – RNS ARITHMETIC

- **Ciphertexts are pairs of polynomials:**
  - Degree is fixed by the parameter N
  - Coefficients are integers modulo q (T_q-bits size)

- **RNS arithmetic:**

  Residue representation accordingly to a basis of co-prime elements.

- **Characteristics:**
  - Introduce distributed parallelism
  - Single precision modular arithmetic
  - Non-positional system (dynamic range handling, complex divisions…)
  - Base extension operation depends on the basis sizes ($O(l^2)$)

HANDLING LARGE COEFFICIENT SIZES

CHINESE REMAINDER THEOREM – RNS ARITHMETIC

- **Ciphertexts are pairs of polynomials:**
  - Degree is fixed by the parameter N
  - Coefficients are integers modulo q (T_q-bits size)

- **RNS arithmetic:**

  Residue representation accordingly to a basis of co-prime elements.

- **Characteristics:**
  - Introduce distributed parallelism
  - Single precision modular arithmetic
  - Non-positional system (dynamic range handling, complex divisions…)
  - Base extension operation depends on the basis sizes ($O(l^2)$)

- **In practice:**
  - RNS basis element: particular primes for efficient modular reduction
  - RNS basis size: $l(T_{primes}) \propto T_q$
  - RNS basis dynamic range $> Max\_value(q)$

RNS arithmetic complexity is under the direct influence of the T_q parameter

- **Residue polynomial multiplication:**
  - Polynomial multiplication over the field $\mathbb{Z}_{p_i}$
  - Polynomial reduction modulo $\Phi(X)$ (degree $N = 2^k$) over the field $\mathbb{Z}_{p_i}$

IMPROVING POLYNOMIAL MULTIPLICATIONS

NTT-BASED RESIDUE POLYNOMIAL MULTIPLICATIONS

- **Residue polynomial multiplication:**
  - Polynomial multiplication over the field $\mathbb{Z}_{p_i}$
  - Polynomial reduction modulo $\Phi(X)$ (degree $N = 2^k$) over the field $\mathbb{Z}_{p_i}$
- **NTT-based polynomial multiplication:**

  Number Theoretical Transform (Fourier transform over finite fields).

- **Characteristics:**
  - Cooley-Tuckey algorithm for NTT: $O(N^2) \longrightarrow O(N \log N)$
  - No polynomial reduction (NWC with $\Phi(X) = X^N + 1$)
  - NTT has a large constant complexity (difficult implementation for large N)
  - Needs of precomputed values ($2N + 2$)

IMPROVING POLYNOMIAL MULTIPLICATIONS

NTT-BASED RESIDUE POLYNOMIAL MULTIPLICATIONS

- **Residue polynomial multiplication:**
  - Polynomial multiplication over the field $\mathbb{Z}_{p_i}$
  - Polynomial reduction modulo $\Phi(X)$ (degree $N = 2^k$) over the field $\mathbb{Z}_{p_i}$

- **NTT-based polynomial multiplication:**

  Number Theoretical Transform (Fourier transform over finite fields).

- **Characteristics:**
  - Cooley-Tuckey algorithm for NTT: $O(N^2) \longrightarrow O(N \log N)$
  - No polynomial reduction (NWC with $\Phi(X) = X^N + 1$)
  - NTT has a large constant complexity (difficult implementation for large N)
  - Needs of precomputed values ($2N + 2$)

- **In practice:**
  - Requires that $\Phi(X) = X^N + 1 \Rightarrow N = 2^k$
  - Select p_i function of N: $2N$ divides $(p_i - 1)$

NTT-based polynomial multiplication complexity is under the direct influence of the parameter N

OVERVIEW

PARAMETERS ANALYSIS
SIZE OF HANDLED CIPHERTEXTS

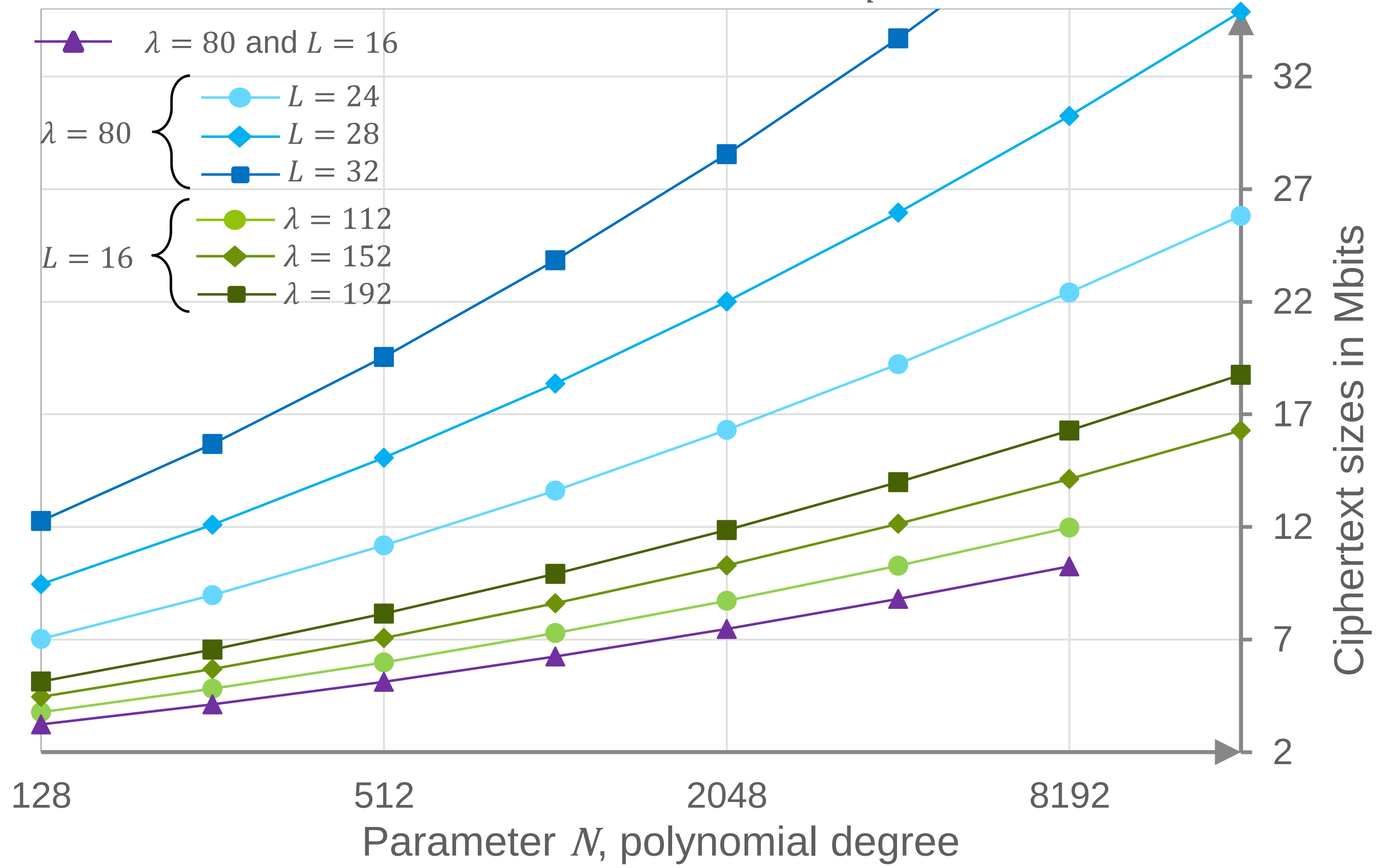
Performances and memory requirements are impacted by ciphertext sizes

$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$

PARAMETERS ANALYSIS
SIZE OF HANDLED CIPHERTEXTS

Performances and memory requirements are impacted by ciphertext sizes

$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$

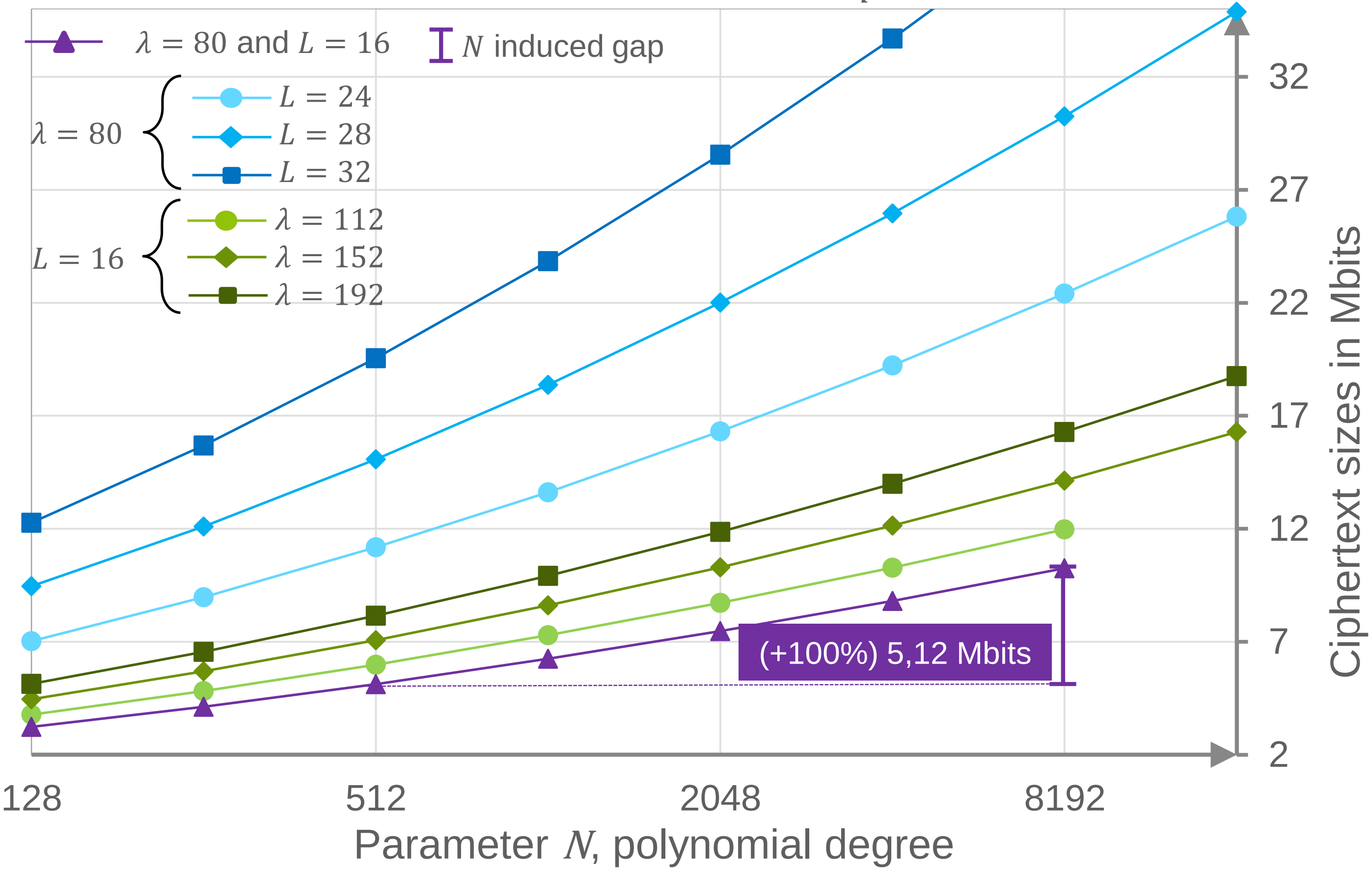


PARAMETERS ANALYSIS

SIZE OF HANDLED CIPHERTEXTS

Performances and memory requirements are impacted by ciphertext sizes

$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$

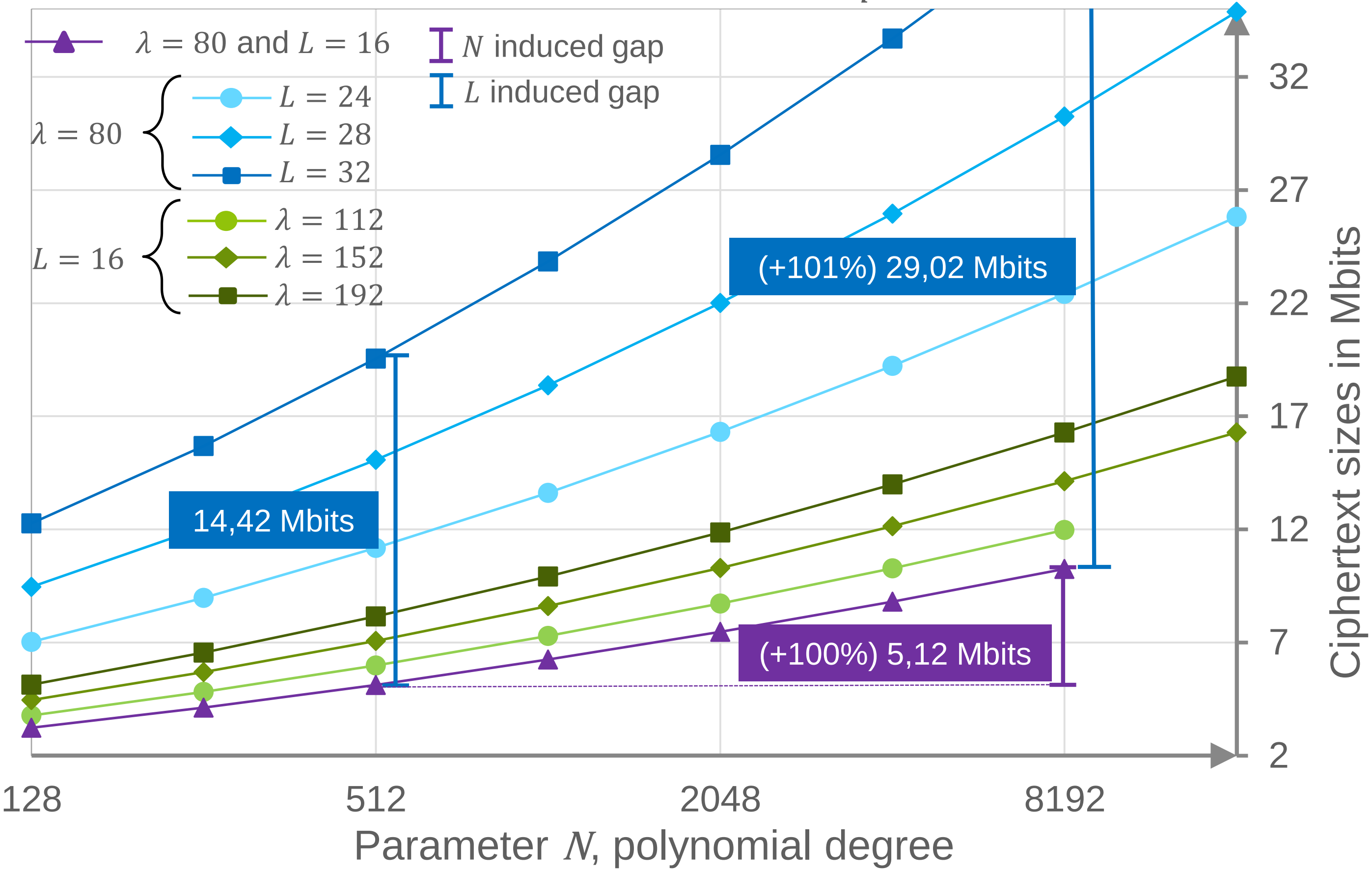


PARAMETERS ANALYSIS

SIZE OF HANDLED CIPHERTEXTS

Performances and memory requirements are impacted by ciphertext sizes

$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$

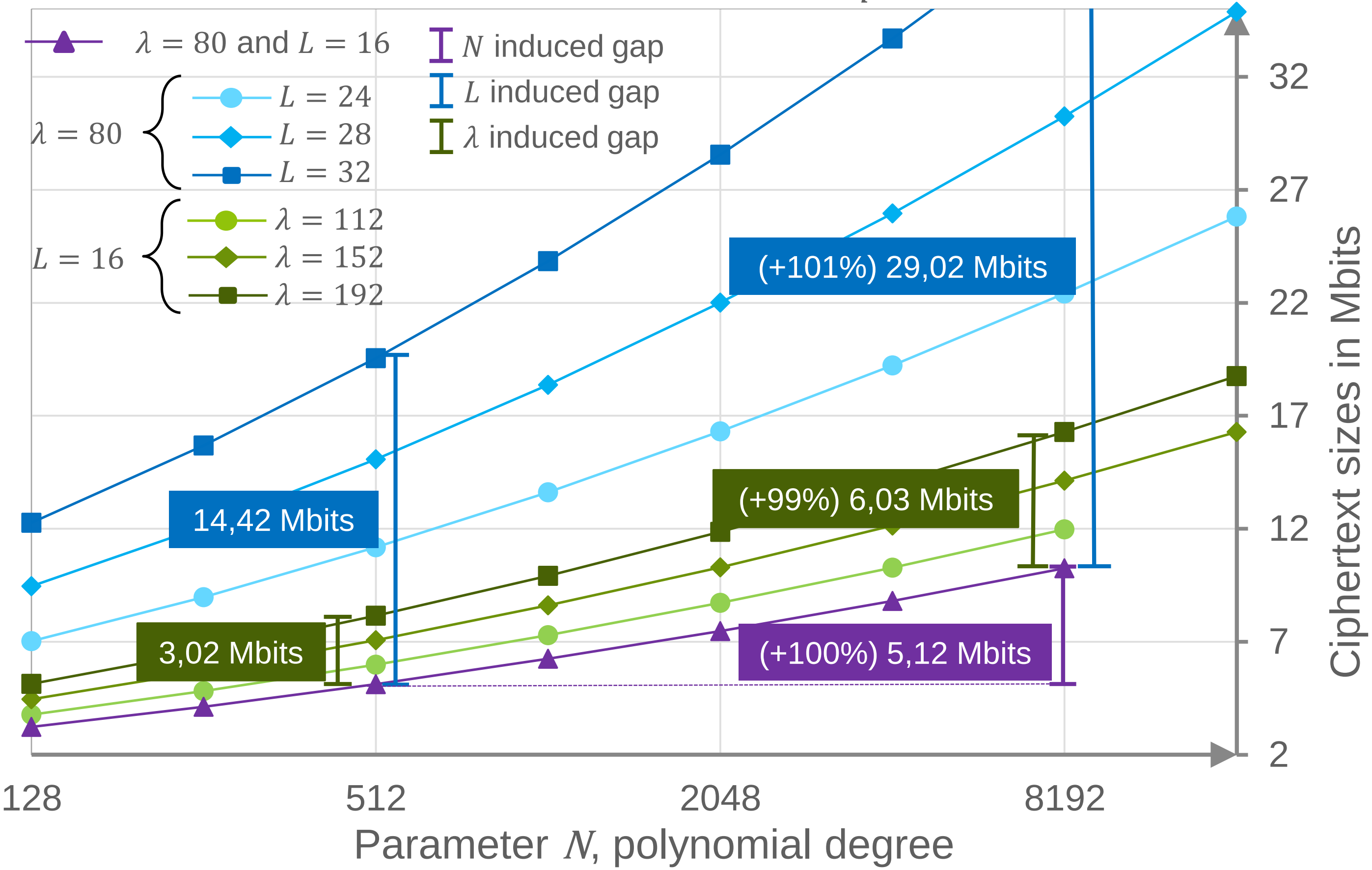


PARAMETERS ANALYSIS

SIZE OF HANDLED CIPHERTEXTS

Performances and memory requirements are impacted by ciphertext sizes

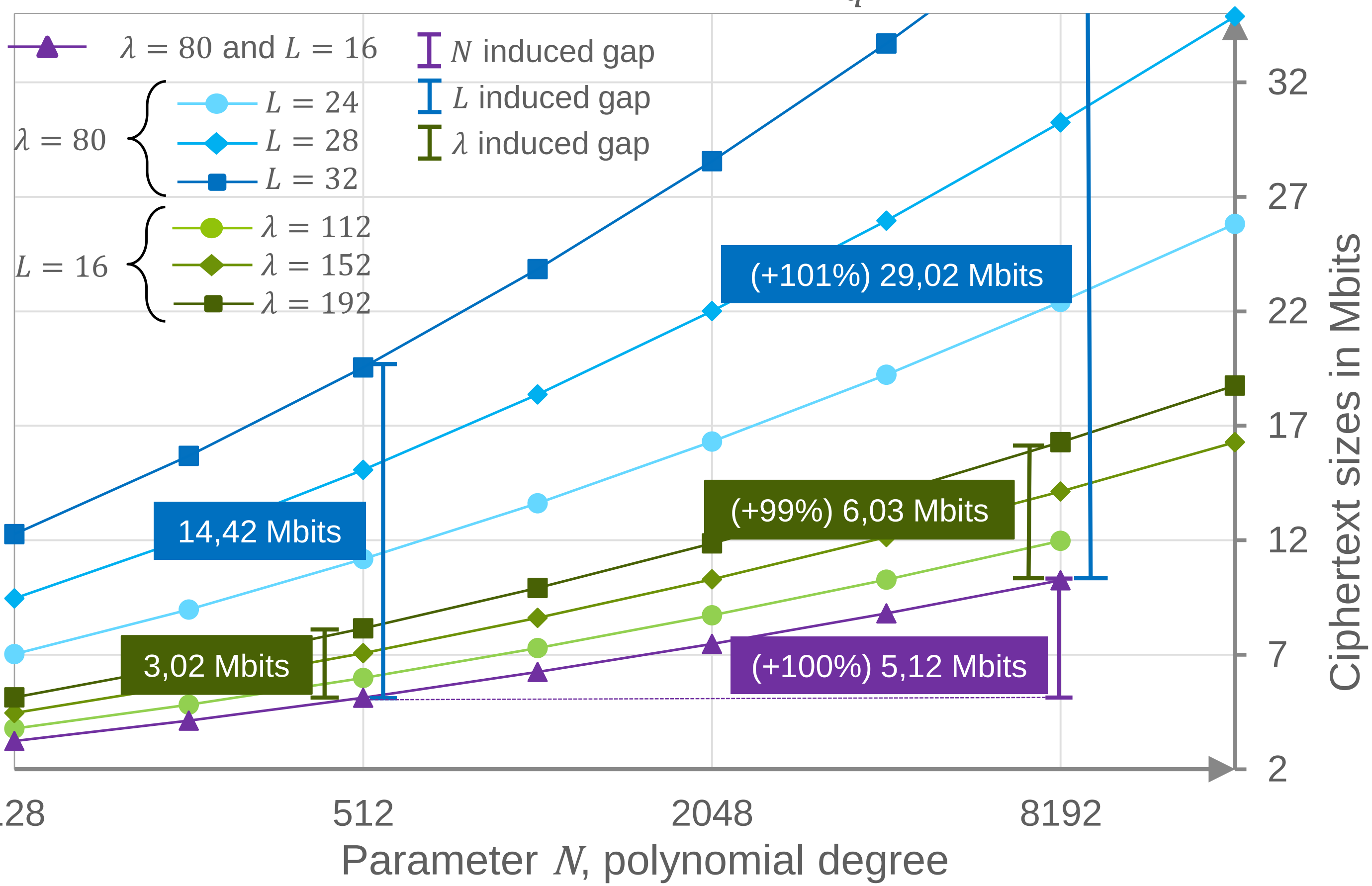
$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$



SIZE OF HANDLED CIPHERTEXTS

Performances and memory requirements are impacted by ciphertext sizes

$$\mathbf{CtxtSize}(\lambda, L, N) = 2 * N * T_q(\lambda, L, N)$$



Not all (N, T_q) are equivalent, smaller N reduce ciphertext sizes

TRADEOFF BETWEEN DEGREE AND COEFFICIENT SIZES

PRIVILEGED SMALL N RATHER THAN SMALL T_q

- **For implementation: small N is better than small T_q**
  - Ciphertexts are smaller
  - More scalable over practical ranges for L and λ
  - Less complex residue polynomial multiplication
  - More parallelism through RNS arithmetic

according to FV'12 derivation rules

- **Limitations in the choice of small N:**
  - Security: lower bound in the lattice dimension?
  - RNS arithmetic:
    - Complexity of base extension $\Longrightarrow$ scale and rounding / modular reduction
    - Availability of RNS base elements

TRADE-OFF BETWEEN DEGREE AND COEFFICIENT SIZES
NUMBER OF PRIMES OF A GIVEN SIZE T_{primes}

$$l_{max} = \left\lceil \frac{5T_q + \log_2 N}{T_{primes}} \right\rceil$$

Choice restrictions

- N-NTT existence over $\mathbb{Z}_{p_i}$
- Efficient reduction mod p_i

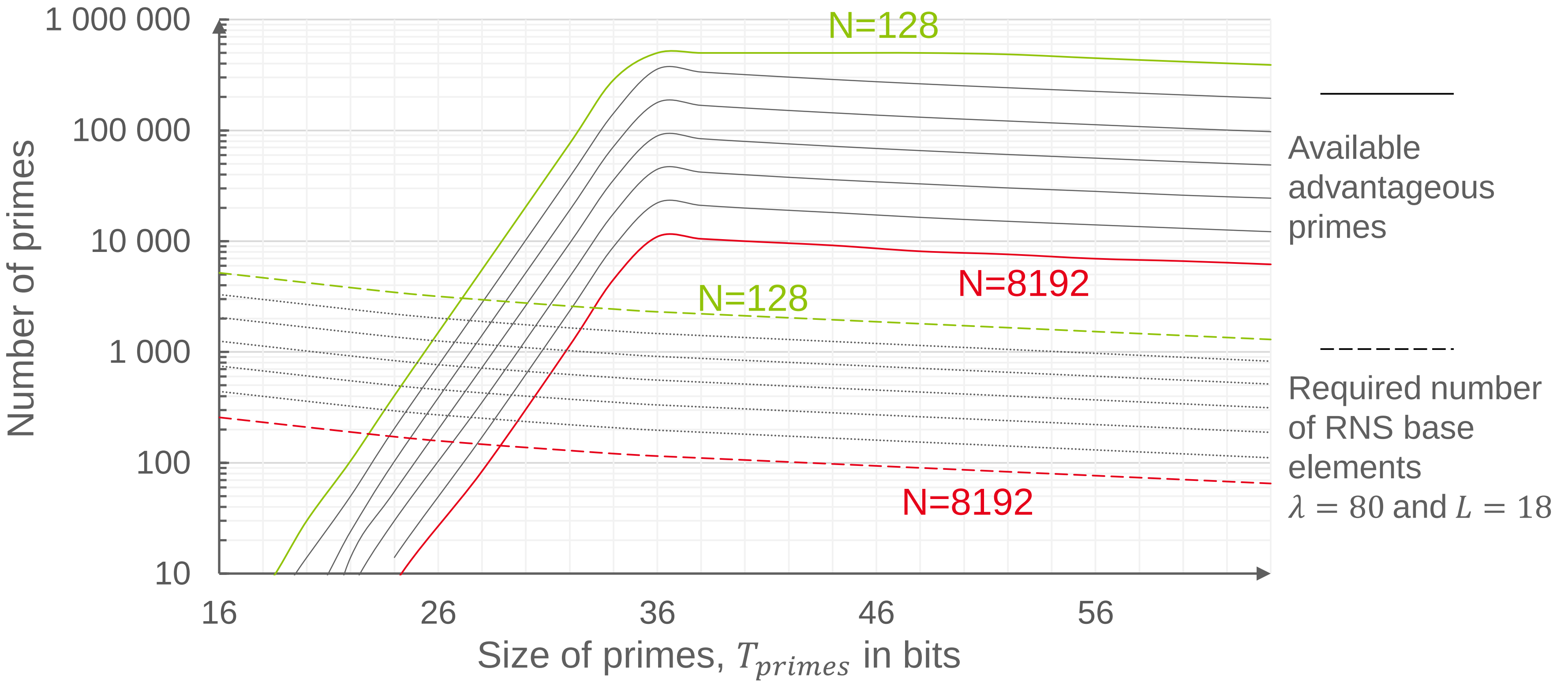
TRADE-OFF BETWEEN DEGREE AND COEFFICIENT SIZES

NUMBER OF PRIMES OF A GIVEN SIZE T_{primes}

$$l_{max} = \left\lceil \frac{5T_q + \log_2 N}{T_{primes}} \right\rceil$$

Choice restrictions
- N-NTT existence over $\mathbb{Z}_{p_i}$
- Efficient reduction mod p_i

Number of advantageous primes found using NFLlib



TRADE-OFF BETWEEN DEGREE AND COEFFICIENT SIZES

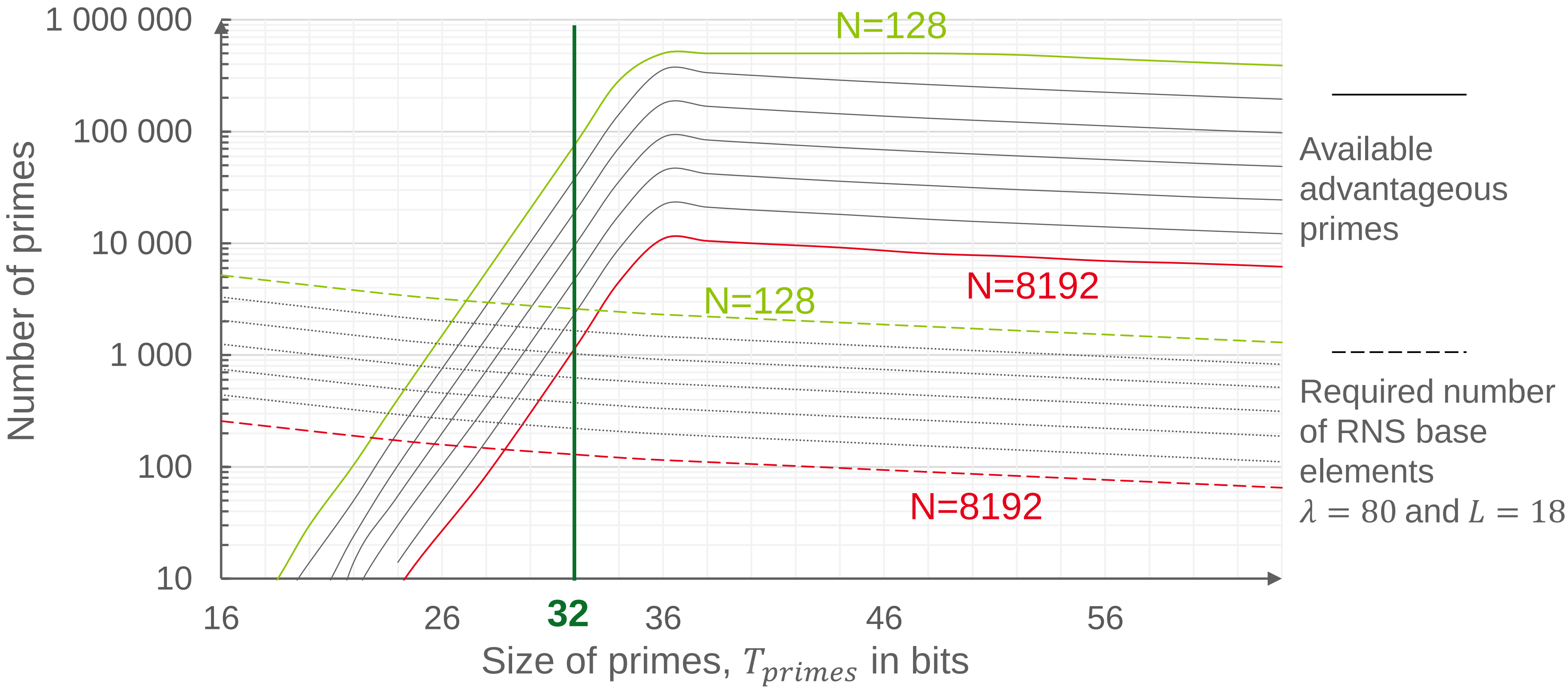
NUMBER OF PRIMES OF A GIVEN SIZE T_{primes}

$$l_{max} = \left\lceil \frac{5T_q + \log_2 N}{T_{primes}} \right\rceil$$

Choice restrictions:

- N-NTT existence over $\mathbb{Z}_{p_i}$
- Efficient reduction mod p_i

Number of advantageous primes found using NFLlib



Regarding practical ranges of (λ, L), we will always have enough advantageous primes

OVERVIEW

CONCLUSION AND PERSPECTIVES

- **Choice of FV parameters is not trivial in practice:**
  - Application: security and multiplicative depth requirements
  - Implementation: complexity, parallelism and memory requirements

- **RNS arithmetic:**
  - Distributed parallelism
  - Complexity ← Base sizes ($\propto T_q$)

- **NTT-based polynomial multiplication:**
  - Limited parallelism (NTT)
  - Costly implementation
  - Complexity ← Degree (N)

- **Results bring by this work:**
  - Regarding FV'12 parameters derivation: small N is clearly advantageous
  - Availability of RNS base elements does not bound the choice of large q

- **Perspectives:**
  - Explore lower bound of N: security / RNS arithmetic complexity
  - Explore experimental hardware complexity regarding N and T_q
  - Exploit the results of this analysis for the design of an hardware accelerator

Thanks!

Do you have some questions?

joel.cathebras@cea.fr

References:

[1] J. Fan and F. Vercauteren, « Somewhat practical fully homomorphic encryption ». IACR Cryptology ePrint Archive, 2012.

[2] Canteaut et al., « Stream ciphers: A practical solution for efficient homomorphic-ciphertext compression ». *Fast Software Encryption*. Springer Nature, 2016.

[3] J-C. Bajard et al., « A Full RNS Variant of FV like Somewhat Homomorphic Encryption Schemes ». Selected Areas in Cryptography – SAC, 2016.

[4] S. Roy et al., « Modular hardware architecture for somewhat homomorphic function evaluation ». *Cryptographic Hardware and Embedded Systems*. Springer, 2015.

[4] C. Aguilar-Melchor et al., « NFLlib: NTT-based fast lattice library ». *Topics in Cryptology*. Springer Nature, 2016.

[6] S. Carpov et al., « Armadillo: A compilation chain for privacy preserving applications ». *Proceedings of the 3rd International Workshop on Security in Cloud Computing*. Association for Computing Machinery (ACM) (2015)

Centre de Saclay
Nano-Innov PC 172 - 91191 Gif sur Yvette Cedex

TRADEOFF BETWEEN DEGREE AND COEFFICIENT SIZES

PRIVILEGED SMALL N RATHER THAN SMALL T_q

- **For implementation: small N is better than small T_q**
  - Ciphertexts are smaller
  - More scalable over practical ranges for L and λ
  - Less complex residue polynomial multiplication
  - More parallelism through RNS arithmetic

according to FV'12 derivation rules

- **Limitations in the choice of small N:**
  - Security: lower bound in the lattice dimension?
  - RNS arithmetic:
    - Complexity of base extension $\Longrightarrow$ scale and rounding / modular reduction
    - Availability of RNS base elements

TRADEOFF BETWEEN DEGREE AND COEFFICIENT SIZES

PRIVILEGED SMALL N RATHER THAN SMALL T_q

- **For implementation:**

Wonderland !!!!

  - Ciphertexts are smaller
  - More scalable over practical ranges for L and λ

according to FV'12 derivation rules

  - Less complex residue polynomial multiplication
  - More parallelism through RNS arithmetic

- **Limitations in the choice of small N:**
  - Security: lower bound in the lattice dimension?
  - RNS arithmetic:
    - Complexity of base extension $\Longrightarrow$ scale and rounding / modular reduction
    - Availability of RNS base elements

TRADEOFF BETWEEN DEGREE AND COEFFICIENT SIZES

PRIVILEGED SMALL N RATHER THAN SMALL T_q

- **For implementation:**

Wonderland !!!!

  - Ciphertexts are smaller
  - More scalable over practical ranges for L and λ
  - Less complex residue polynomial multiplication
  - More parallelism through RNS arithmetic

according to FV'12 derivation rules

- **Limitations in the choice of small N:**
  - Security: lower bound in the lattice dimension?
  - RNS arithmetic:
    - Complexity of base extension $\Longrightarrow$ scale and rounding / modular reduction
    - Availability of RNS base elements

list ceatech

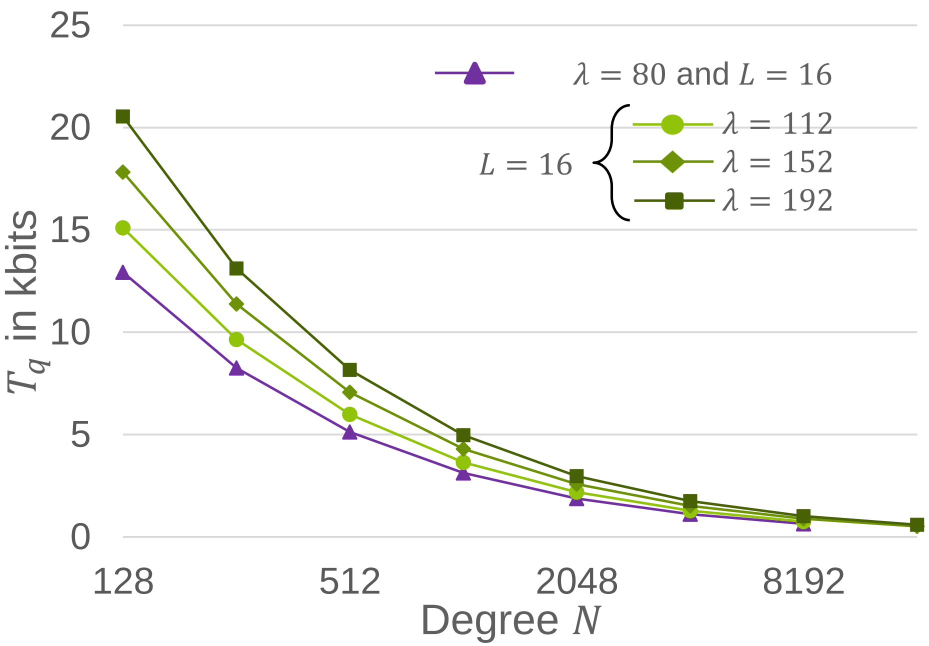
FV PARAMETERS

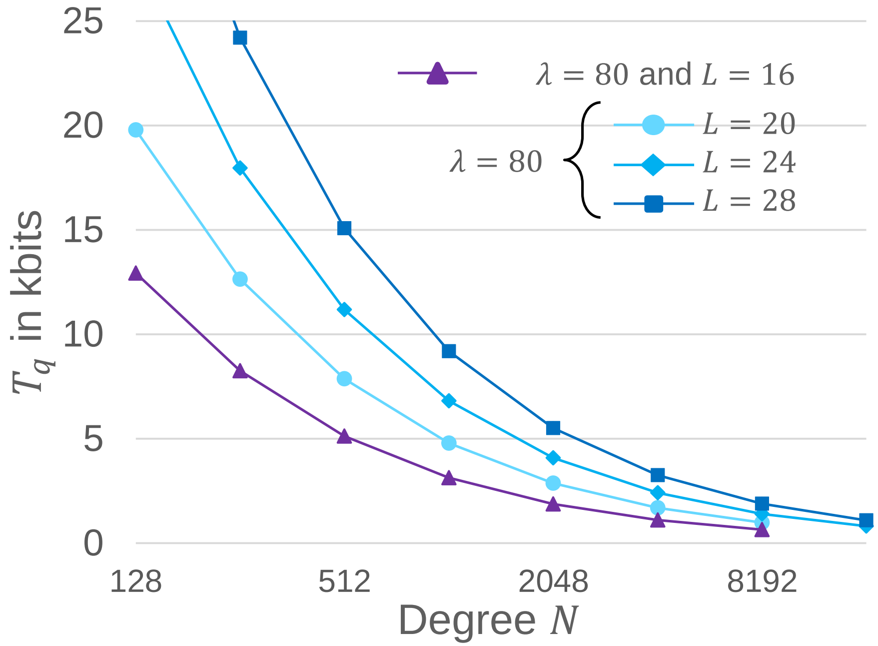
- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**
  - Security level: λ
  - Multiplicative depth: L
  - Plaintext space $(t = 2)$
  - Distinguishing attack ($[\mathrm{LP'11}]$ $\varepsilon = 2^{-64} \Rightarrow \alpha = 3{,}758$)

Derivation

  - Cyclotomic polynomial degree: N (secret Hamming weight $h = 63$)
  - Coefficient sizes: $T_q = \log_2 q$ (parameter σ of the error distribution χ)

- **Relation $T_q(N)$ for fixed (λ, L):**





FV PARAMETERS

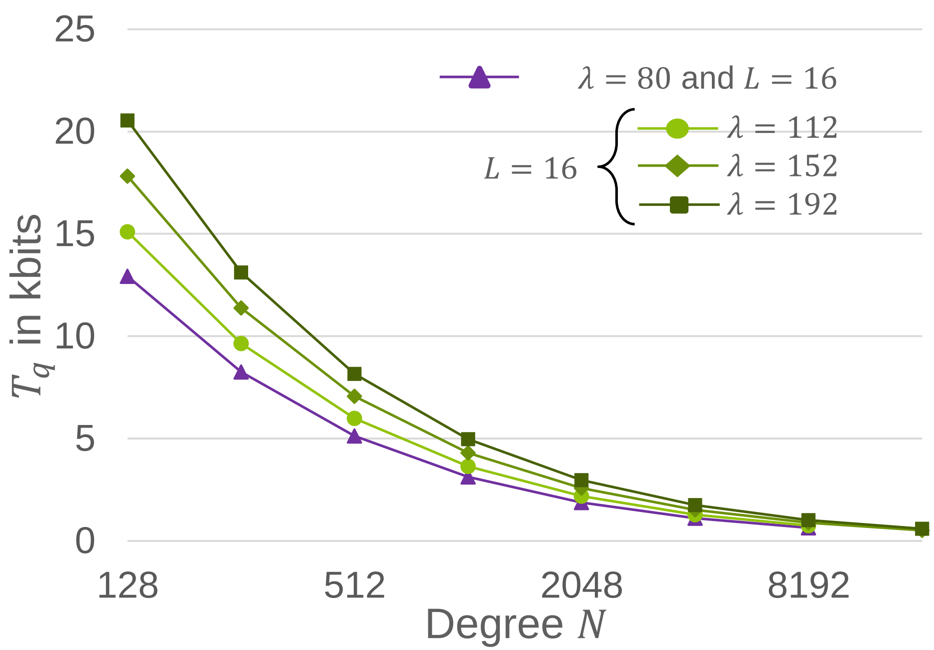
- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**
  - Security level: λ
  - Multiplicative depth: L
  - Plaintext space ($t = 2$)
  - Distinguishing attack ([LP′11] $\varepsilon = 2^{-64} \Rightarrow \alpha = 3{,}758$)

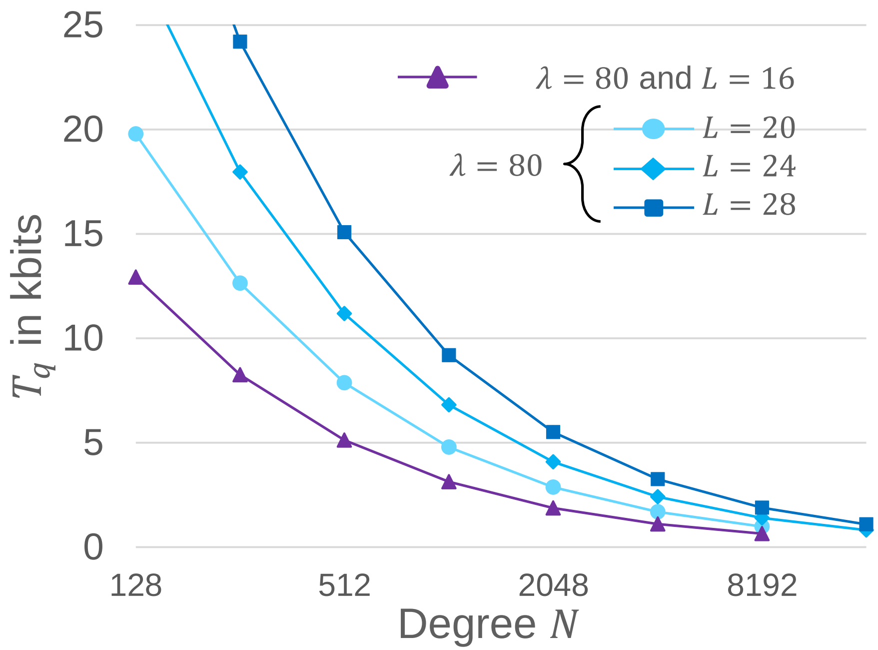
Derivation

[APS’15] ???

  - Cyclotomic polynomial degree: N (secret Hamming weight $h = 63$)
  - Coefficient sizes: $T_q = \log_2 q$ (parameter σ of the error distribution χ)

- **Relation $T_q(N)$ for fixed (λ, L):**





list ceatech

FV PARAMETERS

- **FV instance (λ, L, N, T_q) from J. Fan and F. Vercauteren derivation:**
  - Security level: λ
  - Multiplicative depth: L
  - Plaintext space ($t = 2$)
  - Distinguishing attack ([LP'11] $\varepsilon = 2^{-64} \Rightarrow \alpha = 3{,}758$)

Derivation

[APS'15] ???

  - Cyclotomic polynomial degree: N (secret Hamming weight $h = 63$)
  - Coefficient sizes: $T_q = \log_2 q$ (parameter σ of the error distribution χ)

- **Relation $T_q(N)$ for fixed (λ, L):**