What doctors will use for your prescriptions Between Realism and Paranoia

Carlos Aguilar Melchor, Philippe Gaborit and Javier Herranz

June 1st, 2010

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	?[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	???[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	??????[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	??????????[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	??????????????[Gentry09]

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	??????????????????[Gentry0

What are we talking about (again)?

Group Homomorphic Encryption Scheme

Allows to evaluate monomials or degree 1 polynomials over encrypted data

Fully homomorphic Encryption Schemes

d-multiplicative	degree up to d	[BGN05]
constant-bounded	$\forall d$, d-multiplicative	[AMGH08], [GHV10]
leveled	size: poly(d)	[Gentry09], [vDGHV10]
$\emptyset$	size: $O(1)$	??????????????????????????

[AMGH08]

IACR eprint

Slightly different name ...
Additive Homomorphic Encryption with t-Operand Multiplications
`http://eprint.iacr.org/2008/378`

Eurocrypt 2009, Crypto 2009, Asiacrypt 2009, TCC 2010, ...

To Appear in Crypto'10

Additively Homomorphic Encryption with d-Operand Multiplications

First Interlude

The Cryptographer's Halting Problem

```
Submit Paper to IACR Conference;
While(Paper Rejected)
    Make Corrections;
    Submit to Next IACR Conference;
End While;
```

Distinguish Papers for which this Program Halts

Comparison between [AMGH08] and [Gentry09]

Drawbacks with Respect to [Gentry09]

Multiple layers of encryption

- Leads to an exponential growth on d
- No hope to obtain an alternative independent of d

Advantages

Based on very simple and natural lattice-based schemes

- Almost every lattice-based scheme can be adapted
- Very strong security proofs: classical vs quantum, integer vs ideal
- Relatively small ciphertexts for small values of d

Comparison between [AMGH08] and [Gentry09]

Drawbacks with Respect to [Gentry09]

Multiple layers of encryption

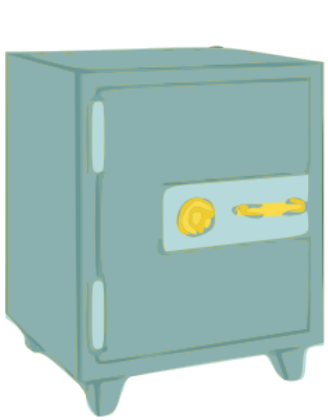
- ~~Leads to an exponential growth on d~~
- No hope to obtain an alternative independent of d

Advantages

Based on very simple and natural lattice-based schemes

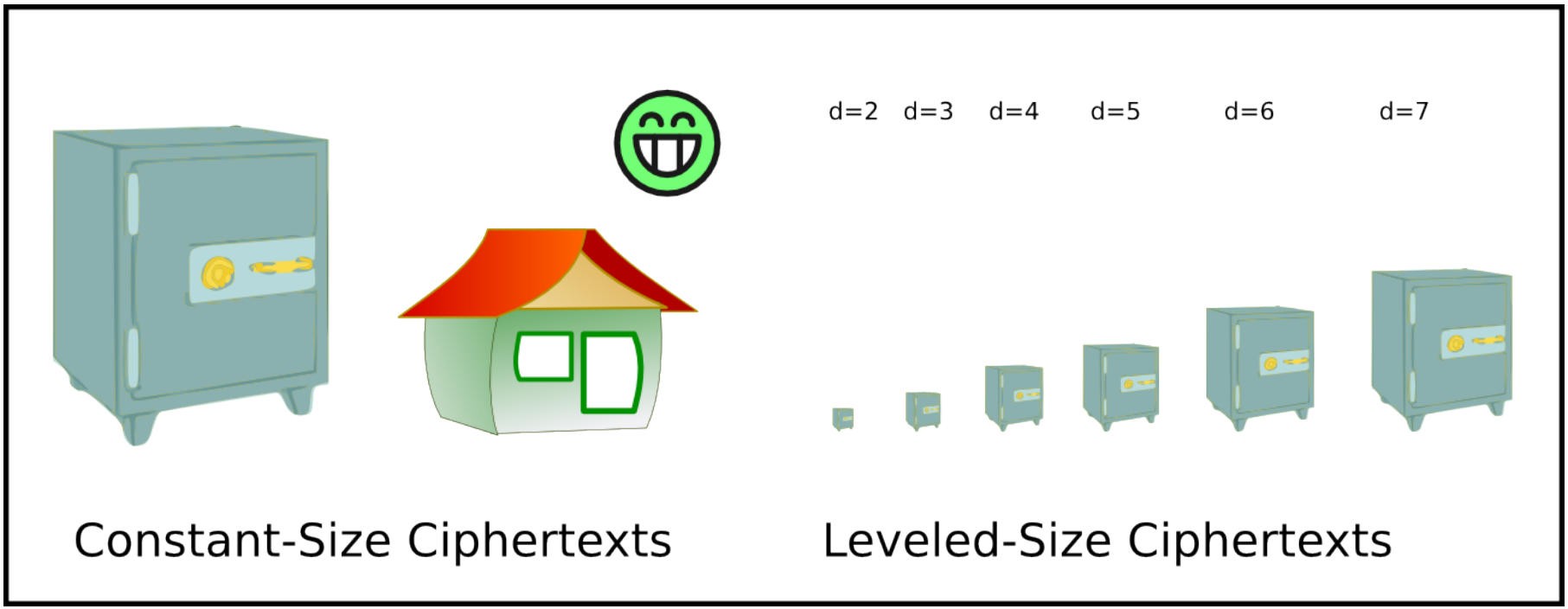
- Almost every lattice-based scheme can be adapted
- Very strong security proofs: classical vs quantum, integer vs ideal
- Relatively small ciphertexts for small values of d

Second Interlude

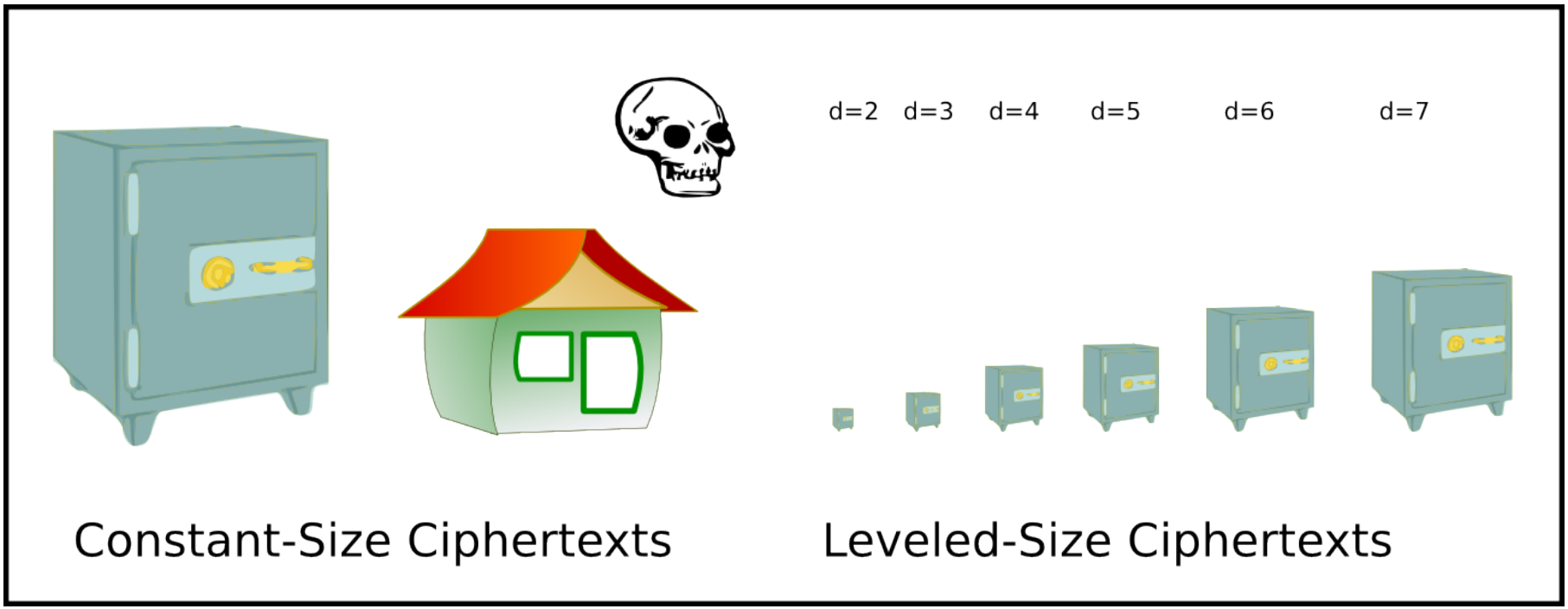


Constant-Size Ciphertexts

Second Interlude



Second Interlude



Alternative construction

From Exponential to Linear Cost (With Worst-Case Hardness Assumptions)

- Crypto 2010: $O(e^d)$
- New Construction: $O(d)$
  - Public Key Instantiation: $\tilde{O}(d^5)$
  - Secret Key Instantiation: $\tilde{O}(d^2)$
- LWE $\Rightarrow$ worst-case hardness for integer lattices
- Ring-LWE $\Rightarrow$ worst-case hardness for ideal lattices over a given ring

Ciphertext Sizes (Symmetric Instantiation)

Polynomial Degree	# Monomials	Ciphertext Size	Lattice dimension
2	100	7 KB	2500
10	10^6	1 MB	25000

To appear (soon) in the IACR eprints