General Impossibility of Group Homomorphic Encryption in the Quantum World

Frederik Armknecht Tommaso Gagliardoni
Stefan Katzenbeisser Andreas Peter

PKC 2014, March 28th
Buenos Aires, Argentina

An example

Consider the basic, unpadded RSA:

- let $N = pq$ for large primes p and q, consider group $(\mathbb{Z}_n^*, \cdot)$
- public exponent e s.t. $\gcd(e, \phi(N)) = 1$
- secret exponent $d = e^{-1} \mod \phi(N)$
- $\mathrm{Enc}(m) = m^e \mod N$ for plaintext m
- $\mathrm{Dec}(c) = c^d \mod N$ for ciphertext c.

An example

Consider the basic, unpadded RSA:

- let $N = pq$ for large primes p and q, consider group $(\mathbb{Z}_n^*, \cdot)$
- public exponent e s.t. $\gcd(e, \phi(N)) = 1$
- secret exponent $d = e^{-1} \mod \phi(N)$
- $\text{Enc}(m) = m^e \mod N$ for plaintext m
- $\text{Dec}(c) = c^d \mod N$ for ciphertext c.

Now consider two plaintexts m_1, m_2, and consider the product of their encryptions:

- $c_1 = \text{Enc}(m_1), c_2 = \text{Enc}(m_2)$
- $\text{Dec}(c_1 \cdot c_2) = \text{Dec}(m_1^e \cdot m_2^e) = \text{Dec}((m_1 \cdot m_2)^e) = (m_1 \cdot m_2)^{ed} \mod N = m_1 \cdot m_2$.

An example

Consider the basic, unpadded RSA:

- let $N = pq$ for large primes p and q, consider group $(\mathbb{Z}_n^*, \cdot)$
- public exponent e s.t. $\gcd(e, \phi(N)) = 1$
- secret exponent $d = e^{-1} \mod \phi(N)$
- $\text{Enc}(m) = m^e \mod N$ for plaintext m
- $\text{Dec}(c) = c^d \mod N$ for ciphertext c.

Now consider two plaintexts m_1, m_2, and consider the product of their encryptions:

- $c_1 = \text{Enc}(m_1), c_2 = \text{Enc}(m_2)$
- $\text{Dec}(c_1 \cdot c_2) = \text{Dec}(m_1^e \cdot m_2^e) = \text{Dec}((m_1 \cdot m_2)^e) = (m_1 \cdot m_2)^{ed} \mod N = m_1 \cdot m_2$.

In this case, decryption is a group homomorphism.

Group Homomorphic Encryption (GHE)

A public-key encryption scheme $\mathcal{E} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ is called group homomorphic if, for any $(pk, sk) \leftarrow \text{Keygen}(\lambda)$:

Group Homomorphic Encryption (GHE)

A public-key encryption scheme $\mathcal{E} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ is called group homomorphic if, for any $(pk, sk) \leftarrow \text{Keygen}(\lambda)$:

- the plaintext space $\mathcal{P}$ is a group in respect to $\otimes$

Group Homomorphic Encryption (GHE)

A public-key encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is called group homomorphic if, for any $(pk, sk) \leftarrow \mathsf{Keygen}(\lambda)$:

- the plaintext space $\mathcal{P}$ is a group in respect to $\otimes$
- the set of encryptions $\mathcal{C} := \left\{ \mathsf{Enc}_{pk}(m; r) | m \in \mathcal{P}, r \in \mathsf{Rnd} \right\}$ is a group in respect to $\star$

Group Homomorphic Encryption (GHE)

A public-key encryption scheme $\mathcal{E} = (\text{KeyGen}, \text{Enc}, \text{Dec})$ is called group homomorphic if, for any $(pk, sk) \leftarrow \text{Keygen}(\lambda)$:

- the plaintext space $\mathcal{P}$ is a group in respect to $\otimes$
- the set of encryptions $\mathcal{C} := \left\{\text{Enc}_{pk}(m; r) | m \in \mathcal{P}, r \in \text{Rnd}\right\}$ is a group in respect to $\star$
- the decryption is a group homomorphism: $\text{Dec}_{sk}(c_1 \star c_2) = \text{Dec}_{sk}(c_1) \otimes \text{Dec}_{sk}(c_2)$, for every $c_1, c_2 \in \mathcal{C}$.

Group Homomorphic Encryption (GHE)

A public-key encryption scheme $\mathcal{E} = (\mathsf{KeyGen}, \mathsf{Enc}, \mathsf{Dec})$ is called group homomorphic if, for any $(pk, sk) \leftarrow \mathsf{Keygen}(\lambda)$:

- the plaintext space $\mathcal{P}$ is a group in respect to $\otimes$
- the set of encryptions $\mathcal{C} := \left\{\mathsf{Enc}_{pk}(m; r) | m \in \mathcal{P}, r \in \mathsf{Rnd}\right\}$ is a group in respect to $\star$
- the decryption is a group homomorphism:
  $\mathsf{Dec}_{sk}(c_1 \star c_2) = \mathsf{Dec}_{sk}(c_1) \otimes \mathsf{Dec}_{sk}(c_2)$, for every $c_1, c_2 \in \mathcal{C}$.

(from now on we will only consider Abelian groups)

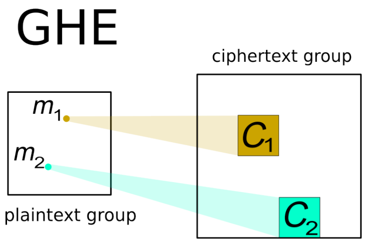
Fully Homomorphic Encryption (FHE)

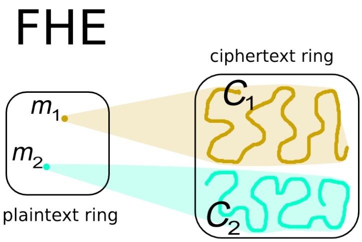
In Fully Homomorphic Encryption we have the following properties:

- plaintext and ciphertext spaces are rings, not just groups (so there are two operations)
- the set of encryptions $\mathcal{C}$ is usually just a set, not necessarily a group
- the decryption is guaranteed to run correctly only after less than $p(\lambda)$ evaluations for some polynomial p.

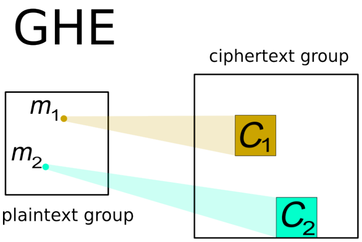
(even if p can be adjusted dynamically through bootstrapping, in GHE the decryption is guaranteed even after unbounded many evaluations)

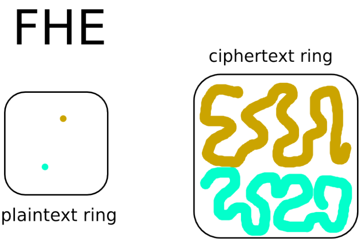
The differences





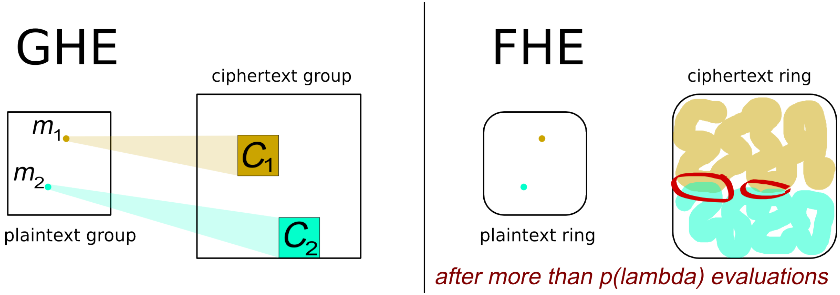
The differences



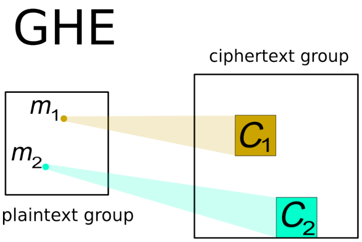


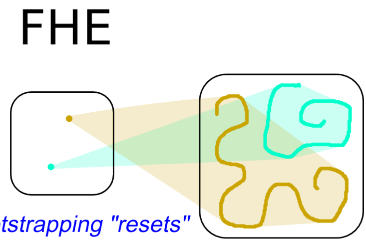
after less than p(lambda) evaluations

The differences



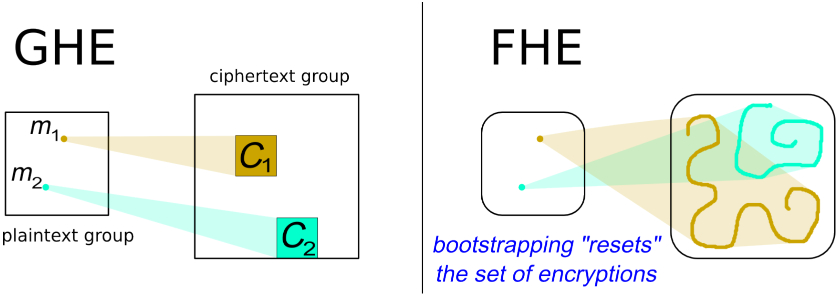
The differences





bootstrapping "resets" the set of encryptions

The differences



GHE is not 'FHE with just one operation': it is something different.

Examples of GHE schemes

RSA
ElGamal
Goldwasser-Micali
Pailler
...

Examples of GHE schemes

RSA
ElGamal
Goldwasser-Micali
Pailler
...

Shor's algorithm

Factorization of integers in quantum PPT.

Examples of GHE schemes

RSA broken
ElGamal
Goldwasser-Micali
Pailler
...

Shor's algorithm

Factorization of integers in quantum PPT.

Examples of GHE schemes

RSA broken
ElGamal
Goldwasser-Micali
Pailler
...

Shor's algorithm

Factorization of integers in quantum PPT.

Watrous' and other variants

Discrete logarithm and many related computational problems in quantum PPT.

Examples of GHE schemes

RSA	broken
ElGamal	broken
Goldwasser-Micali	broken
Pailler	broken
...	

Shor's algorithm

Factorization of integers in quantum PPT.

Watrous' and other variants

Discrete logarithm and many related computational problems in quantum PPT.

Examples of GHE schemes

RSA	broken
ElGamal	broken
Goldwasser-Micali	broken
Pailler	broken
...	

Shor's algorithm

Factorization of integers in quantum PPT.

Watrous' and other variants

Discrete logarithm and many related computational problems in quantum PPT.

Question

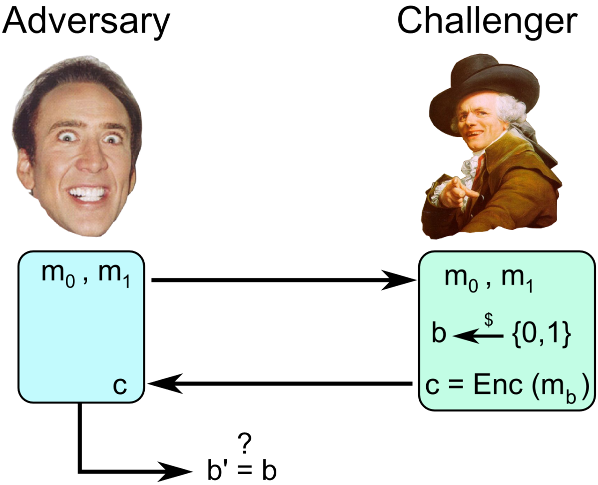
Is GHE possible *at all* in the quantum world?

Our result

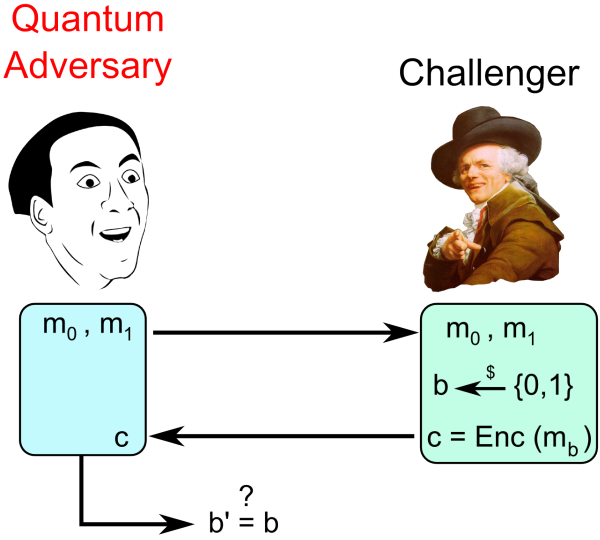
Theorem

Let $\mathcal{E}$ be *any* IND-CPA secure GHE scheme. Then there exists a PPT quantum algorithm which breaks the security of $\mathcal{E}$ with non-negligible probability.

IND-CPA Security



IND-CPA Security



Subgroup Membership Problem (SMP)

Consider a group G and a non-trivial subgroup $H < G$.

Subgroup Membership Problem (SMP)

Consider a group G and a non-trivial subgroup $H < G$.

Given an element $x \in G$ drawn from some distribution:

Problem: decide whether $x \in H$ or $x \in G \setminus H$.

Subgroup Membership Problem (SMP)

Consider a group G and a non-trivial subgroup $H < G$.

Given an element $x \in G$ drawn from some distribution:

Problem: decide whether $x \in H$ or $x \in G \setminus H$.

Remark

In a GHE scheme, the set of encryptions of the neutral element 1_G, $\left\{ \mathsf{Enc}_{pk}(1_G; r) | r \in \mathsf{Rnd} \right\}$ is a subgroup of the ciphertext group.

Subgroup Membership Problem (SMP)

Consider a group G and a non-trivial subgroup $H < G$.

Given an element $x \in G$ drawn from some distribution:

Problem: decide whether $x \in H$ or $x \in G \setminus H$.

Remark

In a GHE scheme, the set of encryptions of the neutral element 1_G, $\left\{\mathrm{Enc}_{pk}(1_G; r) | r \in \mathrm{Rnd}\right\}$ is a subgroup of the ciphertext group.

Theorem

For GHE schemes, IND-CPA security implies hardness of SMP respect to the subgroup of encryptions of 1_G.

notice: vice versa does not hold.

An attack based on Order Finding

Order Finding Problem (OFP): given a non-trivial subgroup $H < G$, find the order (cardinality) of H.

An attack based on Order Finding

Order Finding Problem (OFP): given a non-trivial subgroup $H < G$, find the order (cardinality) of H.

There is a simple way of reducing SMP to OFP. Given $G, H, x \in G$:

1. compute order of H
2. compute order of $\langle H, x \rangle$ (subgroup generated by H and x)
3. $x \in H$ iff the two orders are the same.

An attack based on Order Finding

Order Finding Problem (OFP): given a non-trivial subgroup $H < G$, find the order (cardinality) of H.

There is a simple way of reducing SMP to OFP. Given $G, H, x \in G$:

1. compute order of H
2. compute order of $\langle H, x \rangle$ (subgroup generated by H and x)
3. $x \in H$ iff the two orders are the same.

Watrous' order-finding quantum algorithm

Given generators $g_1, \ldots, g_k$ of subgroup $H < G$, there exists a PPT quantum algorithm which outputs $o(H)$.

An attack based on Order Finding

Order Finding Problem (OFP): given a non-trivial subgroup $H < G$, find the order (cardinality) of H.

There is a simple way of reducing SMP to OFP. Given $G, H, x \in G$:

1. compute order of H
2. compute order of $\langle H, x\rangle$ (subgroup generated by H and x)
3. $x \in H$ iff the two orders are the same.

Watrous' order-finding quantum algorithm

Given generators $g_1, \ldots, g_k$ of subgroup $H < G$, there exists a PPT quantum algorithm which outputs $o(H)$.

Done!

Thanks for your attention!

tommaso@gagliardoni.net

CASED

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

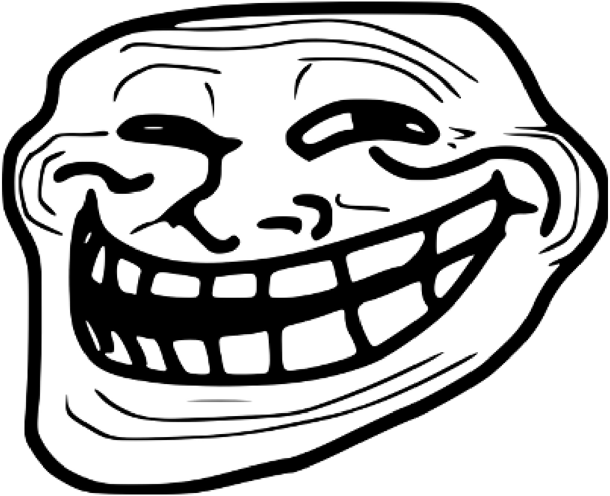
EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

TECHNISCHE
UNIVERSITÄT
DARMSTADT

IN OMNIBUS VERITAS
UNIVERSITÄT MANNHEIM

UNIVERSITY OF TWENTE.

Not so fast...



Not so fast...

What do we mean by a description of a group H?

Not so fast...

What do we mean by a description of a group H?

- a black-box sampling algorithm to sample elements in H

Not so fast...

What do we mean by a description of a group H?

- a black-box sampling algorithm to sample elements in H
- an explicit description of the neutral element

Not so fast...

What do we mean by a description of a group H?

- a black-box sampling algorithm to sample elements in H
- an explicit description of the neutral element
- black-box access to the group operation

Not so fast...

What do we mean by a description of a group H?

- a black-box sampling algorithm to sample elements in H
- an explicit description of the neutral element
- black-box access to the group operation
- black-box access to the inversion of group elements

Not so fast...

What do we mean by a description of a group H?

- a black-box sampling algorithm to sample elements in H
- an explicit description of the neutral element
- black-box access to the group operation
- black-box access to the inversion of group elements

Notice: in GHE, we do not necessary have a set of generators.

The problem

We need a set of generators!!!

The problem

We need a set of generators!!!

Recall: we want to solve the SMP in G in respect to the subgroup of the encryption of 1_G; this would break IND-CPA security.

The problem

We need a set of generators!!!

Recall: we want to solve the SMP in G in respect to the subgroup of the encryption of 1_G; this would break IND-CPA security.

Idea: use the sampling algorithm by requesting encryptions of the neutral element, and hope to find a set of generators after not too many samples.

The uniform case

If the Enc algorithm samples form H according to the uniform distribution, where $ord(H) \leq 2^k$, then:

Theorem [Pak,Bratus,'99]

Sampling $k + 4$ elements yields a generating set for H with probability $\geq \frac{3}{4}$.

The uniform case

If the Enc algorithm samples form H according to the uniform distribution, where $ord(H) \leq 2^k$, then:

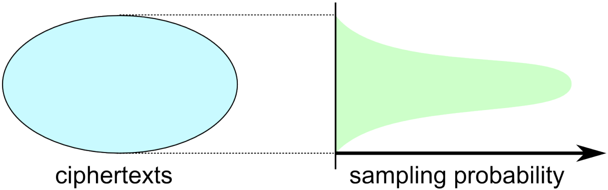
Theorem [Pak,Bratus,'99]

Sampling $k + 4$ elements yields a generating set for H with probability $\geq \frac{3}{4}$.

But in general we can have arbitrary distributions!

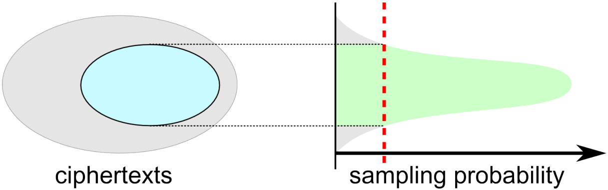
Arbitrary distribution

Much more difficult.



Arbitrary distribution

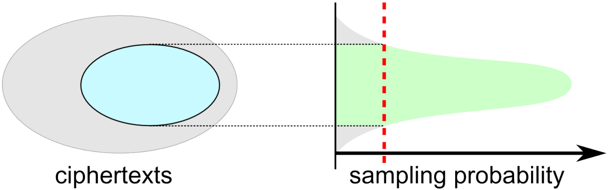
Much more difficult.



Idea: we restrict to a large enough subgroup.

Arbitrary distribution

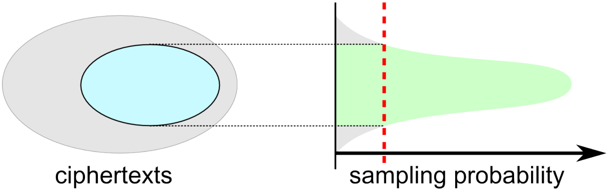
Much more difficult.



Idea: we restrict to a large enough subgroup. Details are tricky

Arbitrary distribution

Much more difficult.



Idea: we restrict to a large enough subgroup. Details are tricky

Theorem

If $H < G$ is a sampleable subgroup according to arbitrary distribution $\mathcal{D}$, with $ord(H) \leq 2^k$, then: sampling $7k \cdot (2 + \lceil \log(k) \rceil) + 1$ elements yields a generating set for H with probability $\approx \frac{3}{4}$, regardless of $\mathcal{D}$.

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$
2. run Watrous' algorithm on $\{c_1, \ldots, c_n\}$, obtaining order o_1

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$
2. run Watrous' algorithm on $\{c_1, \ldots, c_n\}$, obtaining order o_1
3. play the IND-CPA game by choosing $m_0 = 1_G$ and $m_1 \neq 1_G$; receive challenge ciphertext c

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$
2. run Watrous' algorithm on $\{c_1, \ldots, c_n\}$, obtaining order o_1
3. play the IND-CPA game by choosing $m_0 = 1_G$ and $m_1 \neq 1_G$; receive challenge ciphertext c
4. run Watrous' algorithm on $\{c_1, \ldots, c_n, c\}$, obtaining order o_2

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$
2. run Watrous' algorithm on $\{c_1, \ldots, c_n\}$, obtaining order o_1
3. play the IND-CPA game by choosing $m_0 = 1_G$ and $m_1 \neq 1_G$; receive challenge ciphertext c
4. run Watrous' algorithm on $\{c_1, \ldots, c_n, c\}$, obtaining order o_2
5. if $o_1 = o_2$ then output 0, else output 1

The attack

1. generate a large enough number of encryptions of the neutral element 1_G, obtaining $c_1, \ldots, c_n$
2. run Watrous' algorithm on $\{c_1, \ldots, c_n\}$, obtaining order o_1
3. play the IND-CPA game by choosing $m_0 = 1_G$ and $m_1 \neq 1_G$; receive challenge ciphertext c
4. run Watrous' algorithm on $\{c_1, \ldots, c_n, c\}$, obtaining order o_2
5. if $o_1 = o_2$ then output 0, else output 1

Theorem

No GHE scheme can be IND-CPA secure against quantum adversaries.

In the FHE case...

Our attack strictly relies on the group structure.

In the FHE case...

Our attack strictly relies on the group structure.

Sufficient condition: there exist two plaintexts, $m_0 \neq m_1$, and a subgroup H such that:

In the FHE case...

Our attack strictly relies on the group structure.

Sufficient condition: there exist two plaintexts, $m_0 \neq m_1$, and a subgroup H such that:

- we have a PPT algorithm which outputs a small set of generators for H

In the FHE case...

Our attack strictly relies on the group structure.

Sufficient condition: there exist two plaintexts, $m_0 \neq m_1$, and a subgroup H such that:

- we have a PPT algorithm which outputs a small set of generators for H
- the probability that $\mathrm{Enc}(m_0)$ lies in H is high

In the FHE case...

Our attack strictly relies on the group structure.

Sufficient condition: there exist two plaintexts, $m_0 \neq m_1$, and a subgroup H such that:

- we have a PPT algorithm which outputs a small set of generators for H
- the probability that $\mathrm{Enc}(m_0)$ lies in H is high
- the probability that $\mathrm{Enc}(m_1)$ lies in $G \setminus H$ is high

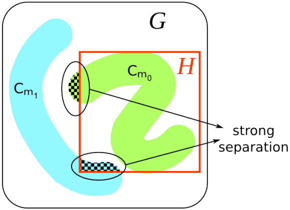
In the FHE case...

Our attack strictly relies on the group structure.

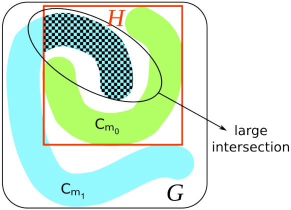
Sufficient condition: there exist two plaintexts, $m_0 \neq m_1$, and a subgroup H such that:

- we have a PPT algorithm which outputs a small set of generators for H
- the probability that $\mathrm{Enc}(m_0)$ lies in H is high
- the probability that $\mathrm{Enc}(m_1)$ lies in $G \setminus H$ is high

Condition fulfilled



Condition not fulfilled



End of this talk (for good...)

Thanks for your attention!

tommaso@gagliardoni.net

CASED

Cryptoplexity
Cryptography & Complexity Theory
Technische Universität Darmstadt
www.cryptoplexity.de

EC SPRIDE
EUROPEAN CENTER FOR
SECURITY AND PRIVACY BY DESIGN

TECHNISCHE
UNIVERSITÄT
DARMSTADT

IN OMNIBUS VERITAS
UNIVERSITÄT MANNHEIM

UNIVERSITY OF TWENTE.