Fully Homomorphic Encryption

Boaz Barak

**Disclaimer:** The MS-Word version of this text has significant formatting issues compared to the PDF and HTML versions.

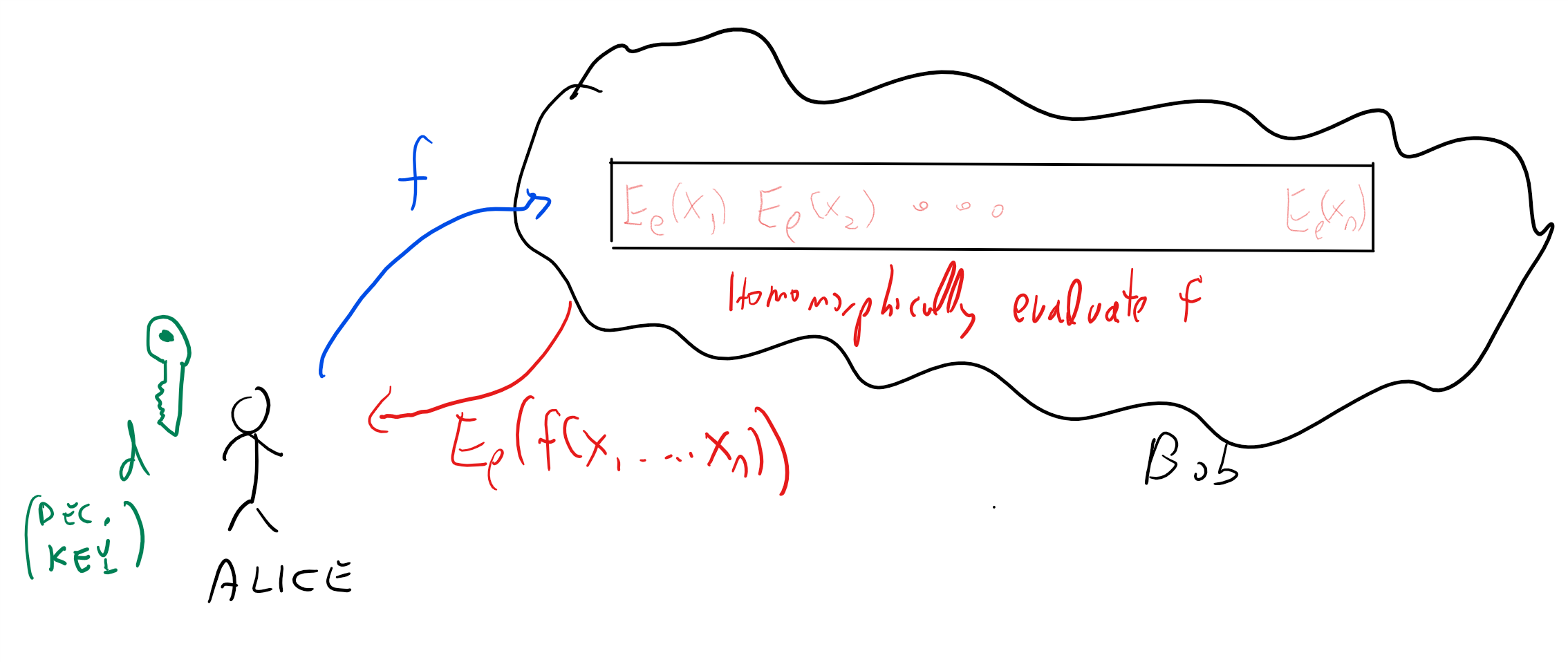
# Fully homomorphic encryption: Introduction and bootstrapping

In today’s era of “cloud computing”, much of individuals’ and businesses’ data is stored and computed on by third parties such as Google, Microsoft, Apple, Amazon, Facebook, Dropbox and many others. Classically, cryptography provided solutions to protecting [data in motion](https://www.schneier.com/blog/archives/2010/06/data_at_rest_vs.html) from point A to point B. But these are not always sufficient to protect [data at rest](https://en.wikipedia.org/wiki/Data_at_rest) and particularly [data in use](https://en.wikipedia.org/wiki/Data_in_use). For example, suppose that *Alice* has some data (in modern applications would well be terabytes in length or larger) that she wishes to store with the cloud service *Bob*, but is afraid that Bob will be hacked, subpoenaed or simply does not completely trust Bob.

Encryption does not seem to immediately solve the problem. Alice could store at Bob an *encrypted* version of the data and keep the secret key for herself. But then she would be at a loss if she wanted to do with the data anything more than retrieving particular blocks of it. If she wanted to outsource computation to Bob as well, and compute for some function , then she would need to share the secret key with Bob, thus defeating the purpose of encrypting the data in the first place.

For example, after the computing systems of Office of Personell Management (OPM) were [discovered to be hacked](https://www.lawfareblog.com/why-opm-hack-far-worse-you-imagine) in June of 2015, revealing sensitive information, including fingerprints and all data gathered during security clearance checks of up to 18 million people, DHS assistant secretary for cybersecurity and communications Andy Ozment [said](http://www.federaltimes.com/story/government/omr/opm-cyber-report/2015/06/19/opm-breach-encryption/28985237/) that encryption wouldn’t have helped preventing it since “if an adversary has the credentials of a user on the network, then they can access data even if it’s encrypted, just as the users on the network have to access data”. So, can we encrypt data in a way that still allows some access and computing on it?

Already in 1978, [Rivest, Adleman and Dertouzos](http://luca-giuzzi.unibs.it/corsi/Support/papers-cryptography/RAD78.pdf) considered this problem of a business that wishes to use a “commercial [time-sharing](https://en.wikipedia.org/wiki/Time-sharing) service” to store some sensitive data. They envisioned a potential solution for this task which they called a privacy homomorphism. This notion later became known as *fully homomorphic encryption (FHE)* which is an encryption that allows a party (such as the cloud provider) that *does not know the secret key* to modify a ciphertext encrypting to a ciphertext encrypting for every efficiently computable . In particular in our scenario above (see fhefig), such a scheme will allow Bob, given an encryption of , to compute the encryption of and send this ciphertext to Alice without ever getting the secret key and so without ever learning anything about (or for that matter).



A fully homomorphic encryption can be used to store data on the cloud in encrypted form, but still have the cloud provider be able to evaluate functions on the data in encrypted form (without ever learning either the inputs or the outputs of the function they evaluate).

Unlike the case of a trapdoor function, where it only took a year for Diffie and Hellman’s challenge to be answered by RSA, in the case of fully homomorphic encryption for more than 30 years cryptographers had no constructions achieving this goal. In fact, some people suspected that there is something inherently incompatible between the security of an encryption scheme and the ability of a user to perform all these operations on ciphertexts. Stanford cryptographer Dan Boneh used to joke to incoming graduate students that he will immediately sign the thesis of anyone who came up with a fully homomorphic encryption. But he never expected that he will actually encounter such a thesis, until in 2009, Boneh’s student Craig Gentry released a [paper](https://crypto.stanford.edu/craig/) doing just that. Gentry’s paper shook the world of cryptography, and instigated a flurry of research results making his scheme more efficient, reducing the assumptions it relied on, extending and applying it, and much more. In particular, Brakerski and Vaikuntanathan managed to obtain a fully homomorphic encryption scheme based only on the *Learning with Error (LWE)* assumption we have seen before.

Although there is an [open source library](http://shaih.github.io/HElib/), as well as [other](https://www.dcsec.uni-hannover.de/fileadmin/ful/mitarbeiter/brenner/wahc14_RC.pdf) [implementations](https://eprint.iacr.org/2014/816), there is still much work to be done in order to turn FHE from theory to practice. For a comparable level of security, the encryption and decryption operations of a fully homomorphic encryption scheme are several orders of magnitude slower than a conventional public key system, and (depending on its complexity) homomorphically evaluating a circuit can be significantly more taxing. However, this is a fast evolving field, and already since 2009 significant optimizations have been discovered that reduced the computational and storage overhead by many orders of magnitudes. As in public key encryption, one would imagine that for larger data one would use a “hybrid” approach of combining FHE with symmetric encryption, though one might need to come up with tailor-made symmetric encryption schemes that can be efficiently evaluated.[[1]](#footnote-35)

In this lecture and the next one we will focus on the fully homomorphic encryption schemes that are *easiest to describe*, rather than the ones that are most *efficient* (though the efficient schemes share many similarities with the ones we will talk about). As is generally the case for lattice based encryption, the current most efficient schemes are based on *ideal* lattices and on assumptions such as ring LWE or the security of the NTRU cryptosystem.[[2]](#footnote-37)

# 

To take the distance between theory and practice in perspective, it might be useful to consider the case of *verifying computation*. In the early 1990’s researchers (motivated initially by zero knowledge proofs) came up with the notion of [probabilistically checkable proofs (PCP’s)](http://madhu.seas.harvard.edu/papers/2009/pcpcacm.pdf) which could yield in principle extremely succinct ways to check correctness of computation.

Probabilistically checkable proofs can be thought of as “souped up” versions of NP completeness reductions and like these reductions, have been mostly used for *negative* results, especially since the initial proofs were extremely complicated and also included enormous hidden constants. However, with time people have slowly understood these better and made them more efficient (e.g., see [this survey](http://m.cacm.acm.org/magazines/2015/2/182636-verifying-computations-without-reexecuting-them/fulltext)) and it has now reached the point where these results, are [nearly practical](http://cacm.acm.org/magazines/2016/2/197429-pinocchio/abstract) (see also [this](https://eprint.iacr.org/2016/646)) and in fact these ideas underly at least one [startup](http://z.cash). Overall, constructions for verifying computation have improved by at least 20 orders of magnitude over the last two decades. (We will talk about some of these constructions later in this course.) If progress on fully homomorphic encryption follows a similar trajectory, then we can expect the road to practical utility to be very long, but there is hope that it’s not a “bridge to nowhere”.

# 

Since large scale fully homomorphic encryption is still impractical, people have been trying to achieve at least weaker security goals using certain assumptions. In particular Intel chips have so called [“Secure enclaves”](https://goo.gl/HW4pPU) which one can think of as a somewhat tamper-protected region of the processor that is supposed to be out of reach for the outside world. The idea is that a cloud provider client would treat this enclave as a trusted party that it can communicate with through the cloud provider. The client can store their data on the cloud encrypted with some key , and then set up a secure channel with the enclave using an authenticated key exchange protocol, and send over. Then, when the client sends over a function to the cloud provider, the latter party can simulate FHE by asking the enclave to compute the encryption of given the encryption of . In this solution ultimately the private key does reside on the cloud provider’s computers, and the client has to trust the security of the enclave. In practice, this could provide reasonable security against remote hackers, but (unlike FHE) probably not against sophisticated attackers (e.g., governments) that have physical access to the server.

## Defining fully homomorphic encryption

We start by defining *partially homomorphic* encryption. We focus on encryption for single bits. This is without loss of generality for CPA security (CCA security is anyway ruled out for homomorphic encryption- can you see why?), though there are more efficient constructions that encrypt several bits at a time.

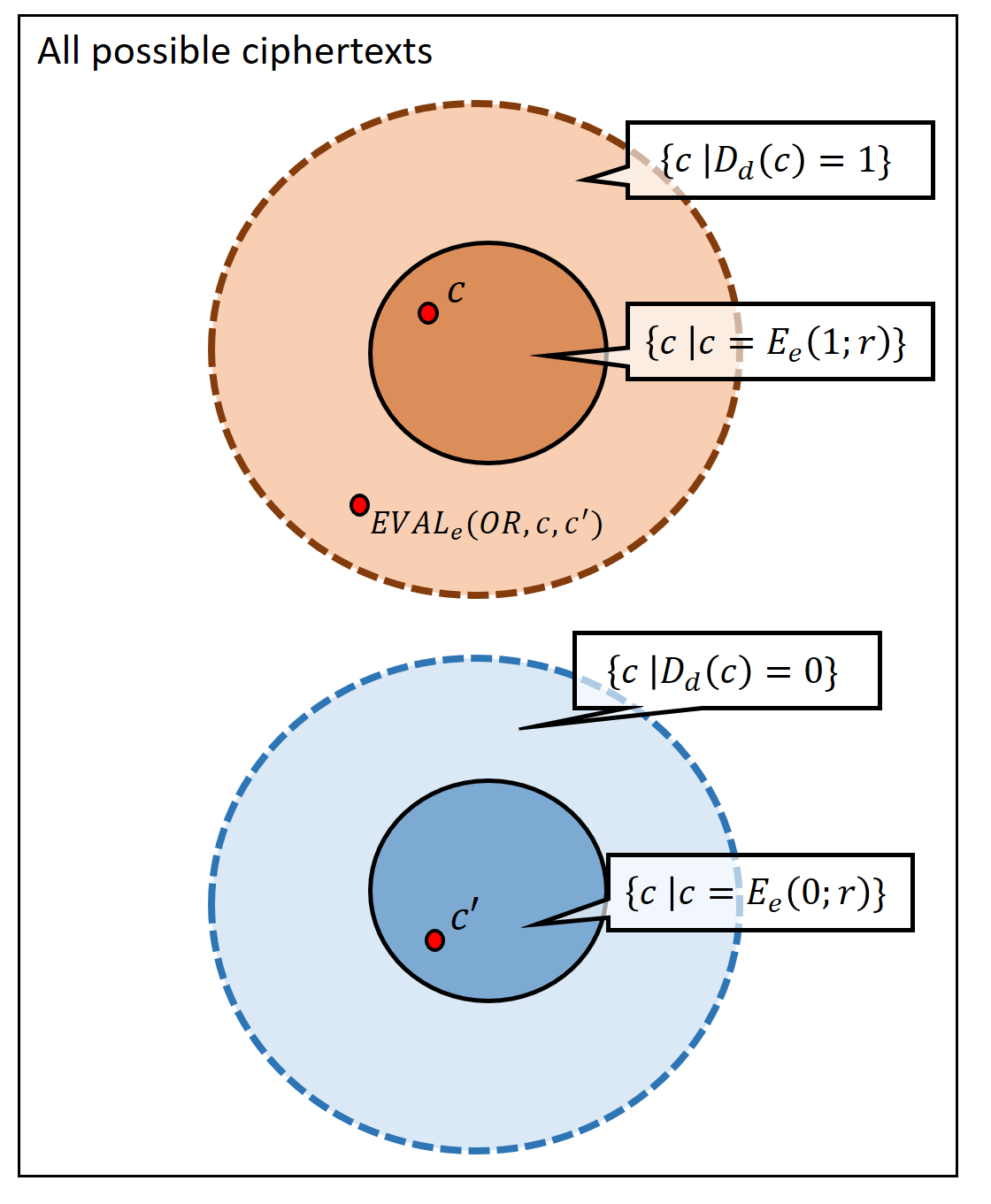
# 

Let be a class of functions where every maps to .  
An *-homomorphic public key encryption scheme* is a CPA secure public key encryption scheme such that there exists a polynomial-time algorithm such that for every , , , and of description size at most it holds that:

* has length at most .
* .

# 

Please stop and verify you understand the definition. In particular you should understand why some bound on the length of the output of is needed to rule out trivial constructions that are the analogous of the cloud provider sending over to Alice the entire encrypted database every time she wants to evaluate a function of it. By artificially increasing the randomness for the key generation algorithm, this is equivalent to requiring that for some fixed polynomial that does not grow with or . You should also understand the distinction between ciphertexts that are the output of the encryption algorithm on the plaintext , and ciphertexts that decrypt to , see evalciphertextfig.



In a valid encryption scheme , the set of ciphertexts such that is a superset of the set of ciphertexts such that for some where is the number of random bits used by the encryption algorithm. Our definition of partially homomorphic encryption scheme requires that for every in our family and , if for then is in the superset of . For example if we apply to the function and ciphertexts that were obtained as encryptions of and respectively, then the output is a ciphertext that would be decrypted to , even if is not in the smaller set of possible outputs of the encryption algorithm on . This distinction between the smaller and larger set is the reason why we cannot automatically apply the function to ciphertexts that are obtained from the outputs of previous operations.

A *fully homomomorphic encryption* is simply a partially homomorphic encryption scheme for the family of *all* functions, where the description of a function is as a circuit (say composed of [NAND](https://en.wikipedia.org/wiki/NAND_gate) gates, which are known to be a universal basis).

### Another application: fully homomorphic encryption for verifying computation

The canonical application of fully homomorphic encryption is for a client to store encrypted data on a server, send a function to the server, and get back the encryption of . This ensures that the server does not learn any information about , but does not ensure that it actually computes the correct function!

Here is a cute protocol to achieve the latter goal (due to [Chung Kalai and Vadhan](https://eprint.iacr.org/2010/241)). Curiously the protocol involves “doubly encrypting” the input, and homomorphically evaluating the function itself.

* **Assumptions:** We assume that all functions that the client will be interested in can be described by a string of length .
* **Preprocessing:** The client generates a pair of keys . In the initial stage the client computes the encrypted database and sends to the server. It also computes for some function as well as for some function and keeps for herself, where is the circuit evaluation function.
* **Client query:** To ask for an evaluation of , the client generates a new random FHE keypair , chooses and lets and . It sends the triple to the server.
* **Server response:** Given the queries , the server defines the function where (for the fixed received) and computes where . (Please pause here and make sure you understand what this step is doing! Note that we use here crucially the fact that itself is a polynomial time computation.)
* **Client check:** Client checks whether and if so accepts as the answer.

We claim that if the server cheats then the client will detect this with probability . Working this out is a great exercise. The probability of detection can be amplified to using appropriate repetition, see the paper for details.

## Example: An XOR homomorphic encryption

It turns out that Regev’s LWE-based encryption LWEENC we saw before is homomorphic with respect to the class of linear (mod 2) functions. Let us recall the LWE assumption and the encryption scheme based on it.

# 

Let be some function mapping the natural numbers to primes. The *-decision learning with error (-dLWE) conjecture* is the following: for every there is a distribution over pairs such that:

* is an matrix over and satisfies and for every .
* The distribution where is sampled from is computationally indistinguishable from the uniform distribution of matrices over .

The *LWE conjecture* is that -dLWE holds for every that is at most . This is not exactly the same phrasing we used before, but can be shown to be essentially equivalent to it.

# 

It is a good idea for you to pause here and try to show the equivalence on your own.

The reason the two conjectures are equivalent are the following. Before we phrased the conjecture as recovering from a pair where and for every . We then showed a *search to decision* reduction (LWEsearchtodecthm) demonstrating that this is equivalent to the task of distinguishing between this case and the case that is a random vector. If we now let and , and consider the matrix and the column vector we see that . Note that if is a random vector in then so is and so the current form of the conjecture follows from the previous one. (To reduce the number of free parameters, we fixed to equal ; in this form the conjecture becomes stronger as grows.)

**A linearly-homomorphic encryption scheme:** We can describe the encryption scheme LWEENC presented in class as:

* Key generation: Choose from where satisfies .
* To encrypt , choose and output
* To decrypt , output iff , where for we defined .

The decryption algorithm recovers the original plaintext since and . It turns out that this scheme is homomorphic with respect to the class of *linear functions* modulo . Specifically we make the following claim:

# 

For every , there is an algorithm that on input encrypting via LWEENC bits , outputs a ciphertext encrypting .

# 

This claim is not hard to prove, but working it out for yourself can be a good way to get more familiarity with LWEENC and the kind of manipulations we’ll be making time and again in the constructions of many lattice based cryptographic primitives. Try to show that (where addition is done as vectors in ) will be the encryption .

# 

The proof is quite simple. will simply add the ciphertexts as vectors in . If then

where is a “noise term” such that . Since , adding at most terms of this difference adds at most , and so we can also write

for . If is even then is an integer multiple of and hence in this case . If is odd and so in this case .

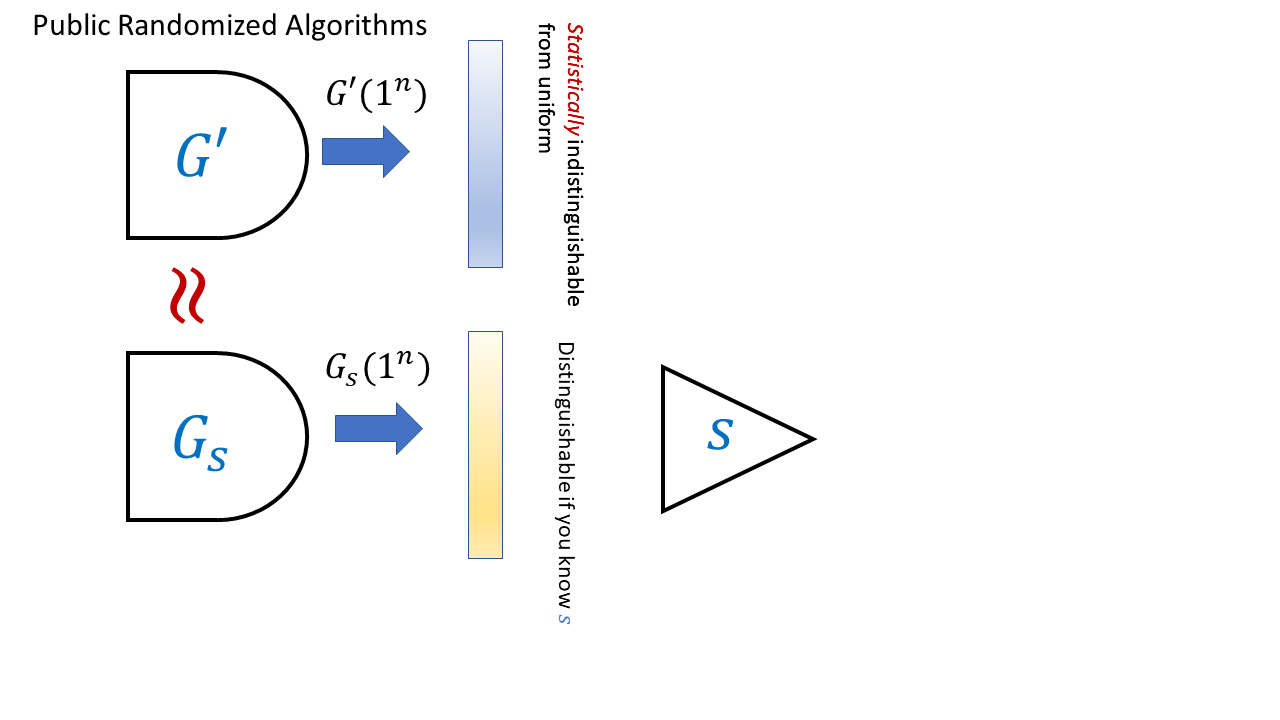
Several other encryption schemes are also homomorphic with respect to linear functions, and even before Gentry’s construction people have managed to achieve homomorphism with respect to slightly larger classes (e.g., quadratic functions by Boneh, Goh and Nissim) but not significantly so.

### Abstraction: A trapdoor pseudorandom generator.

It is instructive to consider the following abstraction (which we’ll use in the next lecture) of the above encryption scheme as a *trapdoor generator* (see TDPgenfig). On input key generation algorithm outputs a vector with and a probabilistic algorithm such that the following holds:

* Any polynomial number of samples from the distribution is computationally indistinguishable from independent samples from the uniform distribution over
* If is output by then .

Thus can be thought of a “trapdoor” for the generator that allows to distinguish between a random vector (that with high probability would satisfy ) and an output of the generator. We use to encrypt a bit by letting and outputting . In the particular instantiation above we obtain by sampling the matrix from the LWE assumption and having output for a random , but we can ignore this particular implementation detail in the forgoing.



In a *trapdoor generator*, we have two ways to generate randomized algorithms. That is, we have some algorithms and such that outputs a pair and outputs with being themselves algorithms (e.g., randomized circuits). The conditions we require are that **(1)** the descriptions of the circuits and (considering them as distributions over strings) are computationally indistinguishable and **(2)** the distribution is *statistically indistinguishable* from the uniform distribution , **(3)** there is an efficient algorithm that given the secret “trapdoor” can distinguish the output of from the uniform distribution. In particular **(1)**,**(2)**, and **(3)** together imply that it is *not* feasible to exract from the description of .

Note that this trapdoor generator satisfies the following stronger property: we can generate an alternative generator such that the description of is indistinguishable from the description of but such that actually does produce (up to exponentially small statistical error) the uniform distribution over . We can define trapdoor generators formally as follows

# 

A *trapdoor generator* is a pair of randomized algorithms that satisfy the following:

* On input , outputs a pair where is a string describing a *randomized* circuit that itself takes as input and outputs a string of length where is some polynomial.
* On input , outputs where is a string describing a randomized circuit that itself takes as input.
* The distributions (i.e., the first output of and are computationally indistinguishable
* With probability over the choice of output by , the distribution is *statistically indistinguishable* (i.e., within total variation distance) from .
* There is an efficient algorithm such that for every pair output by , (where this probability is over the internal randomness used by on the input ) but .[[3]](#footnote-68)

# 

This is not an easy definition to parse, but looking at TDPgenfig can help. Make sure you understand why gives rise to a trapdoor generator satisfying all the conditions of tdpgendef.

**Aside: trapdoor generators in real life:** In the above we use the notion of a “trapdoor” in the pseudorandom generator as a mathematical abstraction, but generators with actual trapdoors have arisen in practice. In 2007 the National Institute of Standards (NIST) released standards for pseudorandom generators. Pseudorandom generators are the quintessential private key primitive, typically built out of hash functions, block ciphers, and such and so it was surprising that NIST included in the list a pseudorandom generator based on public key tools - the [Dual EC DRBG](https://en.wikipedia.org/wiki/Dual_EC_DRBG) generator based on elliptic curve cryptography. This was already strange but became even more worrying when Microsoft researchers Dan Shumow and Niels Ferguson [showed](http://rump2007.cr.yp.to/15-shumow.pdf) that this generator *could* have a trapdoor in the sense that it contained some hardwired constants that if generated in a particular way, there would be some information that (just like in above) allows to distinguish the generator from random (see here for a [2007 blog post](https://www.schneier.com/blog/archives/2007/11/the_strange_sto.html) on this issue). We learned more about this when leaks from the Snowden document [showed](http://www.reuters.com/article/us-usa-security-rsa-idUSBRE9BJ1C220131220) that the NSA secretly paid 10 million dollars to RSA to make this generator the default option in their Bsafe software.

You’d think that this generator is long dead but it turns out to be the “gift that keeps on giving”. In December of 2015, Juniper systems [announced](http://www.wired.com/2015/12/juniper-networks-hidden-backdoors-show-the-risk-of-government-backdoors/) that they have discovered a malicious code in their system, dating back to at least 2012 (possibly [2008](https://goo.gl/X6pAXV)), that would allow an attacker to surreptitiously decrypt all VPN traffic through their firewalls. The issue is that Juniper has been using the Dual EC DRBG and someone has managed to replace the constant they were using with another one, one that they presumably knew the trapdoor for (see [here](https://rpw.sh/blog/2015/12/21/the-backdoored-backdoor/) and [here](http://blog.cryptographyengineering.com/2015/12/on-juniper-backdoor.html) for more; of course unless you know to check for this, it’s very hard by looking at the code to see that one arbitrary looking constant has been replaced by another). Apparently, even though this is very surprising to many people in law enforcement and government, inserting back doors into cryptographic primitives might end up making them less secure.

## From linear homomorphism to full homomorphism

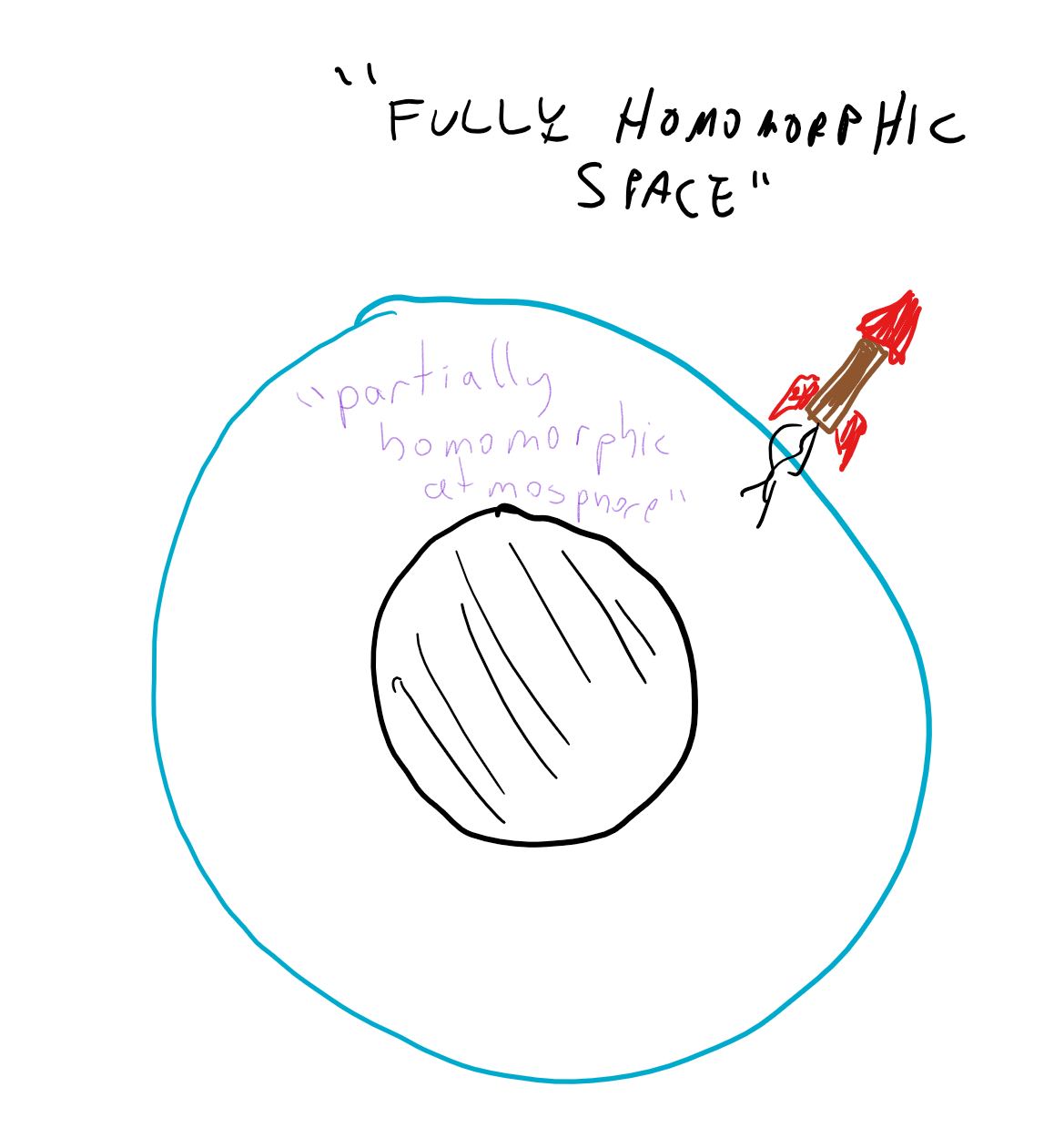
Gentry’s breakthrough had two components:

* First, he gave a scheme that is homomorphic with respect to arithmetic circuits (involving not just addition but also multiplications) of *logarithmic depth*.
* Second, he showed the amazing “bootstrapping theorem” that if a scheme is homomorphic enough to evaluate its own decryption circuit, then it can be turned into a *fully homomorphic* encryption that can evaluate *any* function.

Combining these two insights led to his fully homomorphic encryption.[[4]](#footnote-79)

In this lecture we will focus on the second component - the bootstrapping theorem. We will show a “partially homomorphic encryption” (based on a later work of Gentry, Sahai and Waters) that can fit that theorem in the next lecture.

## Bootstrapping: Fully Homomorphic “escape velocity”



The “Bootstrapping Theorem” shows that once a partially homomorphic encryption scheme is homomorphic with respect to a rich enough family of functions, and specifically a family that contains its own decryption algorithm, then it can be converted to a fully homomorphic encryption scheme that can be used to evaluate *any* function.

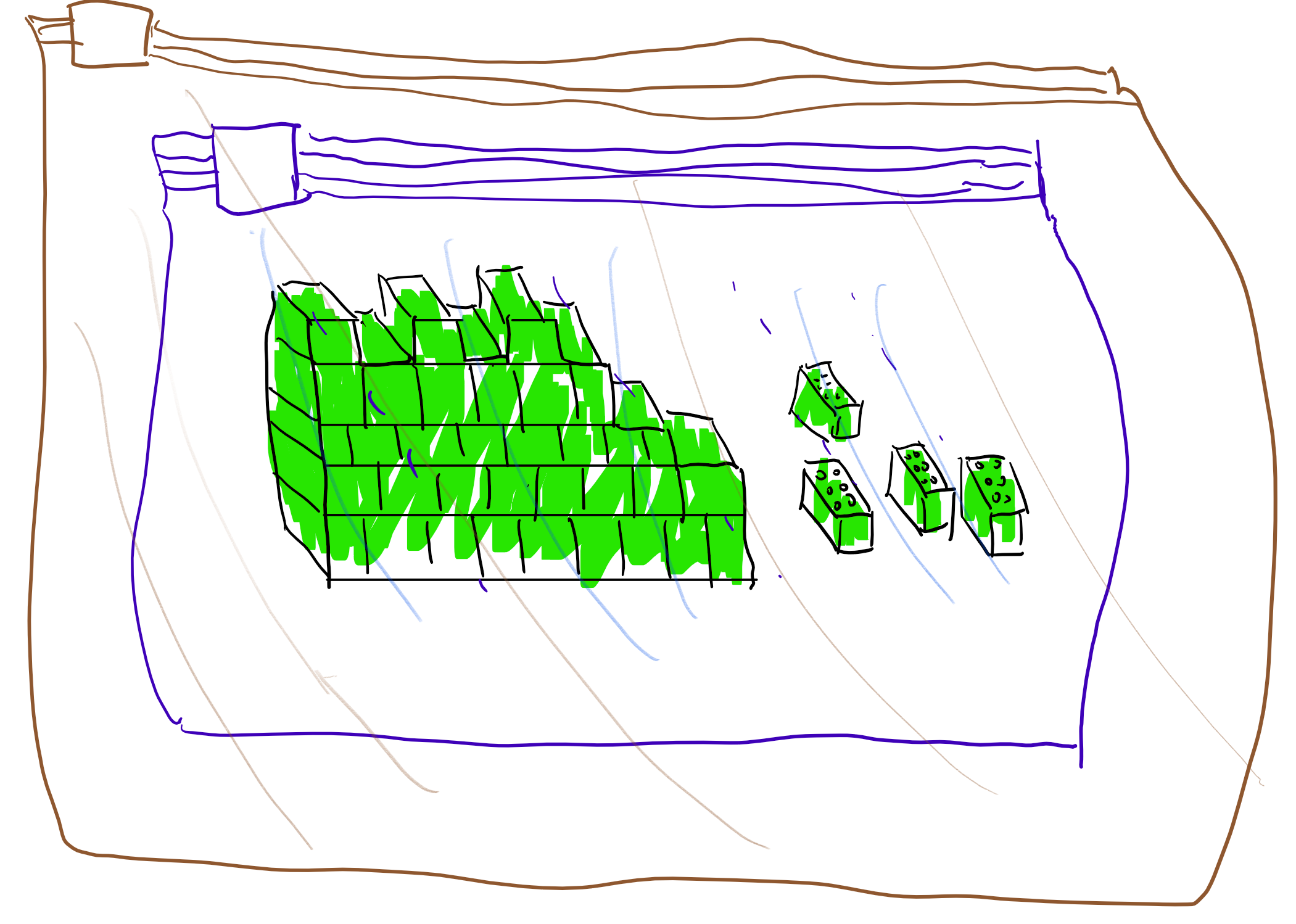
The bootstrapping theorem is quite surprising. A priori you might expect that given that a homomorphic encryption for linear functions was not trivial to do, a homomorphic encryption for quadratics would be harder, cubics even harder and so on and so forth. But it turns out that there is some special degree such that if we obtain homomorphic encryption for degree polynomials then we can obtain *fully* homomorphic encryption that works for *all* functions. (Specifically, if the decryption algorithm is a degree polynomial, then homomorphically evaluating polynomials of degree will be sufficient.) That is, it turns out that once an encryption scheme is strong enough to *homomorphically evaluate its own decryption algorithm* then we can use it to obtain a fully homomorphic encryption by “pulling itself up by its own bootstraps”. One analogy is that at this point the encryption reaches “escape velocity” and we can continue onwards evaluating gates in perpetuity.

We now show the bootstrapping theorem:

# 

Suppose that is a CPA circular[[5]](#footnote-84) secure partially homomorphic encryption scheme for the family and suppose that for every pair of ciphertexts the map is in . Then can be turned a fully homomorphic encryption scheme.

### Radioactive legos analogy



To build a castle from radioactive Lego bricks, which can be kept safe in a special ziploc bag for 10 seconds, we can: 1) Place the bricks in a bag, and place the bag inside an outer bag. 2) Manipulate the inner bag through the outer bag to remove the bricks from it in 9 seconds, and spend 1 second putting one brick in place 3) Now the outer bag has 9 seconds of life left, and we can put it inside a new bag and repeat the process.

Here is one analogy for bootstrapping, inspired by Gentry’s [survey](https://crypto.stanford.edu/craig/easy-fhe.pdf). Suppose that you need to construct some complicated object from a highly toxic material (see ziplocbagfig). You are given a supply of sealed bags that are flexible enough so you can manipulate the object from outside the bag. However, each bag can only hold for seconds of such manipulations before it leaks. The idea is that if you can open one bag inside another within seconds then you can perform the manipulations for arbitrary length. That is, if the object is in the bag then you put this bag inside the bag, spend seconds on opening the bag inside the bag and then spend another second of whatever manipulations you wanted to perform. We then continue this process by putting the bag inside the bag and so on and so forth.

### Proving the bootstrapping theorem

We now turn to the formal proof of bootstrapthm

# 

The idea behind the proof is simple but ingenious. Recall that the NAND gate is a universal gate that allows us to compute any function that can be efficiently computed. Thus, to obtain a fully homomorphic encryption it suffices to obtain a function such that . (Note that this is stronger than the typical notion of homomorphic evaluation since we require that outputs an encryption of when given *any* pair of ciphertexts that decrypt to and respectively, regardless whether these ciphertexts were produced by the encryption algorithm or by some other method, including the procedure itself.)

Thus to prove the theorem, we need to modify into an encryption scheme supporting the operation. Our new scheme will use the same encryption algorithms and but the following modification of the key generation algorithm: after running , we will append to the public key an encryption of the secret key. We have now defined the key generation, encryption and decryption. CPA security follows from the security of the original scheme, where by circular security we refer exactly to the condition that the scheme is secure even if the adversary gets a single encryption of the public key.[[6]](#footnote-91) This latter condition is not known to be implied by standard CPA security but as far as we know is satisfied by all natural public key encryptions, including the LWE-based ones we will plug into this theorem later on.

So, now all that is left is to define the operation. On input two ciphertexts and , we will construct the function (where is the length of the secret key) such that . It would be useful to pause at this point and make sure you understand what are the inputs to , what are “hardwired constants” and what is its output. The ciphertexts and are simply treated as fixed strings and are *not* part of the input to . Rather is a function (depending on the strings ) that maps the secret key into a bit. When running we of course do not know the secret key , but we can still design a circuit that computes this function . Now will simply be defined as . Since , we get that

Thus indeed we map *any* pair of ciphertexts that decrypt to into a ciphertext that decrypts to . This is all that we needed to prove.

# 

Don’t let the short proof fool you. This theorem is quite deep and subtle, and requires some reading and re-reading to truly “get” it.

1. In [2012](https://eprint.iacr.org/2012/099.pdf) the state of art on homomorphically evaluating AES was about six orders of magnitude slower than non-homomorphic AES computation. I don’t know what’s the current record. [↑](#footnote-ref-35)
2. As we mentioned before, as a general rule of thumb, the difference between the ideal schemes and the one that we describe is that in the ideal setting one deals with *structured* matrices that have a compact representation as a single vector and also enable fast FFT-like matrix-vector multiplication. This saves a factor of about in the storage and computation requirements (where is the dimension of the subspace/lattice). However, there can be some subtle security implications for ideal lattices as well, see e.g., [here](https://eprint.iacr.org/2016/127), [here](https://eprint.iacr.org/2015/313), [here](https://eprint.iacr.org/2016/139), and [here](https://eprint.iacr.org/2015/676). [↑](#footnote-ref-37)
3. The choice of is arbitrary, and can be amplified as needed. [↑](#footnote-ref-68)
4. The story is a bit more complex than that. Frustratingly, the decryption circuit of Gentry’s basic scheme was just a little bit too deep for the bootstrapping theorem to apply. A lesser man, such as yours truly, would at this point surmise that fully homomprphic encryption was just not meant to be, and perhaps take up knitting or playing bridge as an alternative hobby. However, Craig persevered and managed to come up with a way to “squash” the decryption circuit so it can fit the bootstrapping parameters. Follow up works, and in particular the paper of Brakerski and Vaikuntanathan, managed to get schemes with much better relation between the homomorphism depth and decryption circuit, and hence avoid the need for squashing and also improve the security assumptions. [↑](#footnote-ref-79)
5. You can ignore the condition of circular security in a first read - we will discuss it later. [↑](#footnote-ref-84)
6. Without this assumption we can still obtained a form of FHE known as a *leveled* FHE where the size of the public key grows with the [depth](https://en.wikipedia.org/wiki/Circuit_complexity) of the circuit to be evaluated. We can do this by having public keys where is the depth we want to evaluate, and encrypt the private key of the key with the public key. However, since circular security seems quite likely to hold, we ignore this extra complication in the rest of the discussion. [↑](#footnote-ref-91)