MPC-FHE Experiments.

Towards next big techs to focus on

CPerezz

Privacy Scaling Explorations (PSE)

Motivation & Goals

Give a SHORT overview of FHE it's usages and some conclusions.

1. Answer basic common questions on FHE and it's related work.
2. See where we have applied FHE so far.
3. See FHE limitations, alternatives etc..
4. Conclusions

FHE - What-Why-How

What

Being able to compute on other's private data.

Encrypted result matches the expected non-encrypted one when decrypted.

Why

Strong primitive that allows for lots of use cases.

PQ-secure SOTA - Good long-term primitive investment security-wise.

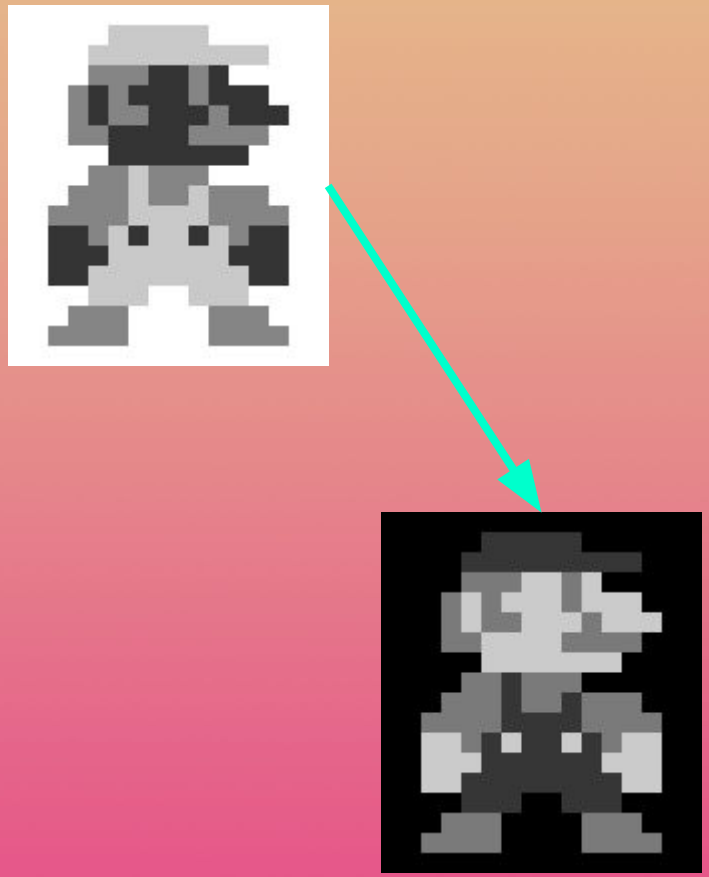
Untrusted TEE.

How

Complex mathematical structures that allow operations on ciphertexts.

Primitives that optimize for these setups.

FHE – What can you build?



[FHE]toshop

- Edit images inside of a Server who doesn't even know what or how is editing.
- Protection against Deep Learning based on your images.
- SASS more appealing when privately editing pictures is guaranteed.

FROGCRYPTO FHE ARENA

(Also known as “let your frogs do something like fighting each other”)

- You can use a Proof of Encryption scheme which proofs the validity of the Frogs.
- You place your frogs strategically considering their different types (as in Pokemon).
- Nor your frogs or strategy are revealed. Yet the winner is elected.
- Allows for really cool things (winner decrypts a signed Tx that allows it to retrieve the opponent’s bet **UNCONDITIONALLY TO ANYTHING ELSE.**

```
let mut frog1: FrogStats<u8> = FrogStats::<T: u8> {
    attack: 10,
    defense: 3,
    health: 5,
};

let mut frog2: FrogStats<u8> = FrogStats::<T: u8> {
    attack: 5,
    defense: 9,
    health: 2,
};

let res: (bool, bool, bool) = battle(f1: &mut frog1, f2: &mut frog2);
```

```
FHE round_damage 17.094818655s
FHE round state updates 15.389155504s
FHE total round 32.483989972s
FHE round_damage 17.132896898s
FHE round state updates 15.388174954s
FHE total round 32.521087525s
FHE round_damage 17.229187171s
FHE round state updates 15.637094161s
FHE total round 32.866297817s
[examples/frog_arena.rs:260:5] out_results = [
    false,
    true,
    false,
]
```

2 Important Lessons Learned

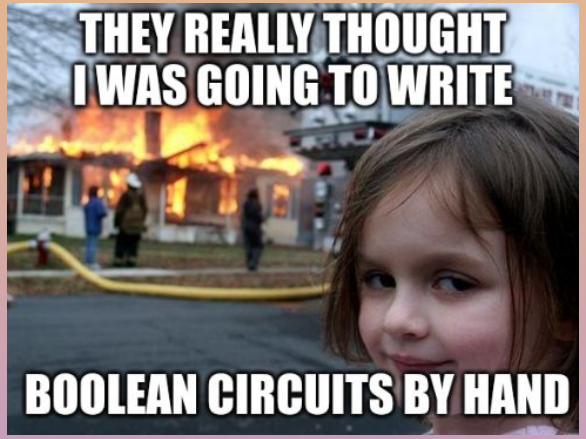
It’s a pain to write by hand + optimize for parallel bootstrapping.

- Found ways to make writing circuits easier (Using C 🤣)
- Found ways to profit from parallelization of boolean gates and bootstrapping reduction.
- Although terribly hacky, **IT WORKED!**

…

…

(Unless when it didn’t)



HEIR: Homomorphic Encryption Intermediate Representation

build passing | contributors 32 | discussions 13 total | license Apache-2.0 | openssf scorecard 6.9

An MLIR-based toolchain for homomorphic encryption compilers. Read the docs at the HEIR website.

For more information on MLIR, see the MLIR homepage.

Demo: HEIR Jupyter Playground

This is a way to start running HEIR compiler passes in a Jupyter notebook or IPython notebook without having to build the entire HEIR project from scratch.

Uses the nightly HEIR build. In this demo, we'll run locally in this github clone to access some external dependencies (e.g. Yosys).

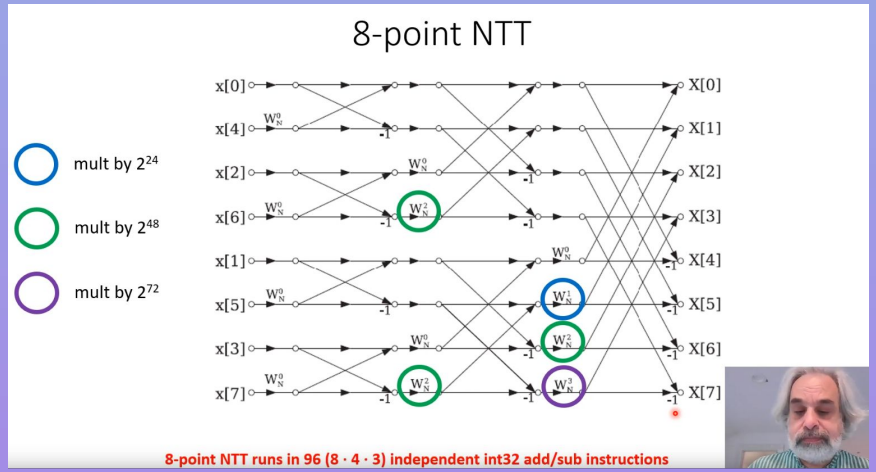
Usage

Load Jupyter in the `scripts/jupyter` notebook:

```
cd scripts/jupyter
python -m venv venv
source venv/bin/activate
pip install -r requirements.txt
jupyter notebook
```

The demo is in Demo.ipynb.

Then connect to your Jupyter runtime and start executing the demo!



Performance

I am running on an RTX 4070 Ti, and I see the best performance with `./gpu_tester 3072 100`, with a run time of 4.713 ms. This is `3*1024*100 / 0.004713` = 65.2 million 1024-point NTTs per second. Note, this performance is achieved by remaining in L2 cache. Global memory bandwidth on my card is about 2.5x too slow to sustain this rate.

If the software were further developed, I believe it should be possible to achieve about 24,000 1M-point NTTs/sec on an RTX 4070 Ti.

Bootstrapping & [NTT/FFT] Speedups

- Already a good state of the art. FFT/NTT are well known colleagues from ZKP/Signal processing world.

- Is by far one of the biggest bottlenecks, and we can compile towards abusing this.

What do we build now?

Private Social Trust graph

- A secret trust graph that anyone can privately query.
- No info is leaked to anyone. Not even the FHE server.
- We get rid of all the communication costs that MPC incurs on.
- We know trust based on how much our trusted ones trust others still.

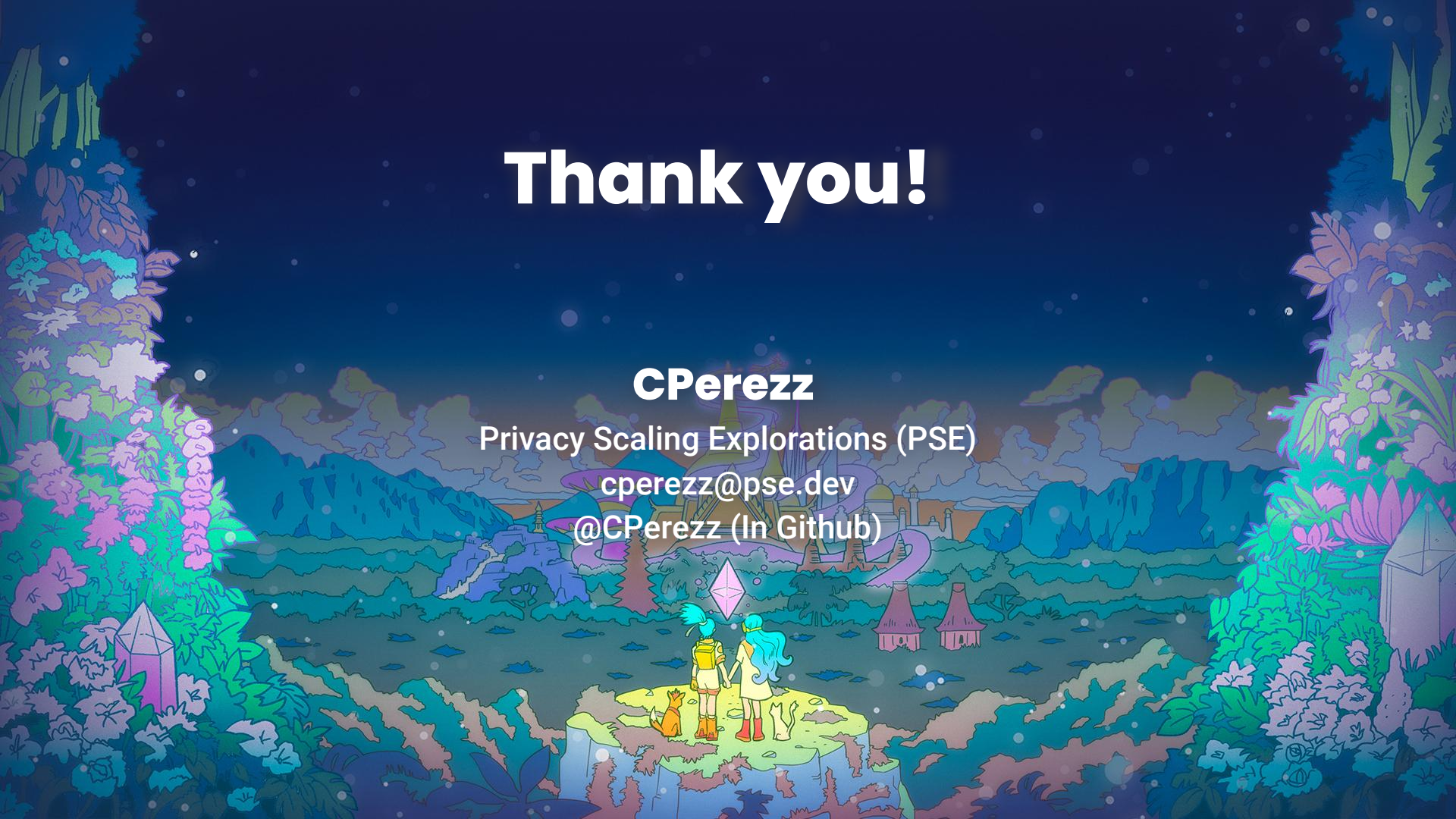
Private Web-Search at civilization scale.

- Stopping the data-mining that society is being a victim of.
- An easy way to bring privacy by default without extra requirements to users.
- Based on PIR over Indexed-DB after PageRank.
- Can be an extra

Questions & Conclusions

Some experimentation time and other explorations lead us to conclude:

- Slow but powerful.
- Superset by other primitives. What's worthier and more powerful?
  - WE & GWE
  - IO
- Is other MPC enough?
- How much can we trick this (Optimizations/Quick Wins)
- How complex is it to find significant theoretical and applicable improvements?


Thank you!
CPerezz
Privacy Scaling Explorations (PSE)
cperezz@pse.dev
@CPerezz (In Github)

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 2 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur. Excepteur sint occaecat cupidatat non proident, sunt in culpa qui officia deserunt mollit anim id est laborum.

Enter your main point / statement here.

Enter your main point / statement here.

Here’s the timeline.

Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”

— Pythagoras

Enter your slide title here

Your slide subtitle here.

Your Name
Your title, your organization

Section 1

Section 1 title here.

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
    - Condimentum
        - Magna
        - Ligula

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 2 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 3

Section 3 title here.

Enter your main point / statement here.

Section 3 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Enter your main point / statement here.

Here’s the timeline.

Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
— Pythagoras

Thank you!

Your Name
Your title, your organization
your@email.address
@youraccount

Enter your slide title here

Your slide subtitle here.

Your Name

Your title, your organization

Section 1

Section 1 title here.

Section 1 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 1 details with an image. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 1 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2

Section 2 title here.

Section 2 title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua.

- Sollicitudin
- Consectetur
  - Condimentum
    - Magna
    - Ligula

Section 2 details with an image.
Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 2 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Section 3

Section 3 title here.

Enter your main point / statement here.

Section 3 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Section 4

Section 4 title here.

Section 4 details with a main point. Enter title here.

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam, quis nostrud exercitation ullamco laboris nisi ut aliquip ex ea commodo consequat. Duis aute irure dolor in reprehenderit in voluptate velit esse cillum dolore eu fugiat nulla pariatur.

Enter your main point / statement here.

Enter your main point / statement here.

Here's the timeline.

Event 1

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 2

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

Event 3

Lorem ipsum dolor sit amet, consectetur adipiscing elit, sed do eiusmod tempor incididunt ut labore et dolore magna aliqua. Ut enim ad minim veniam.

99.99%

“Number rules the universe.”
— Pythagoras

Thank you!

Your Name

Your title, your organization

your@email.address

@youraccount