ABSTRACT WRITING WORKSHOP

(FOR LAY AUDIENCES)

Samuel Pagliarini
Centre for Hardware Security
Dpt. of Computer Systems - School of IT
Tallinn University of Technology

The heck we are talking about in this workshop

- Why would you need training for this? An abstract is an abstract

Generic advice for ACADEMIC abstract

General background

Specific background

Knowledge gap

My contribution

My results

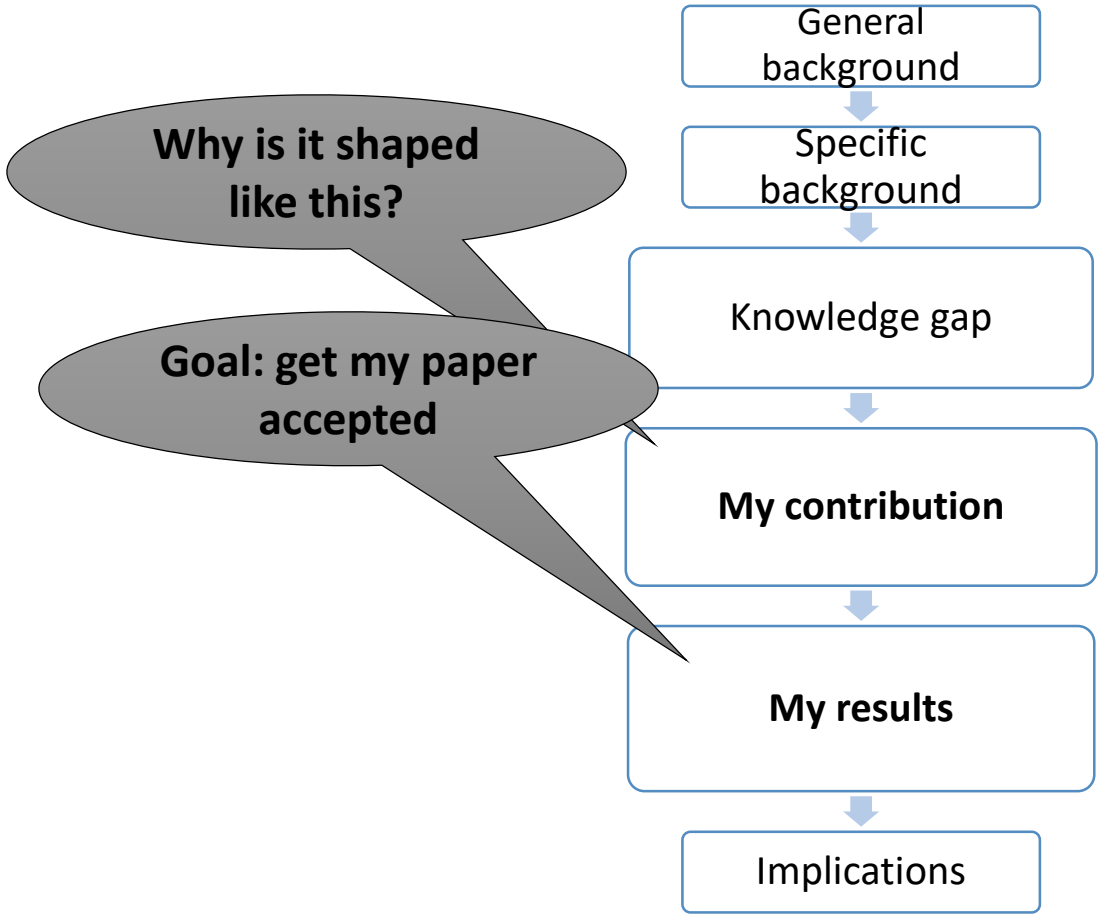
Implications

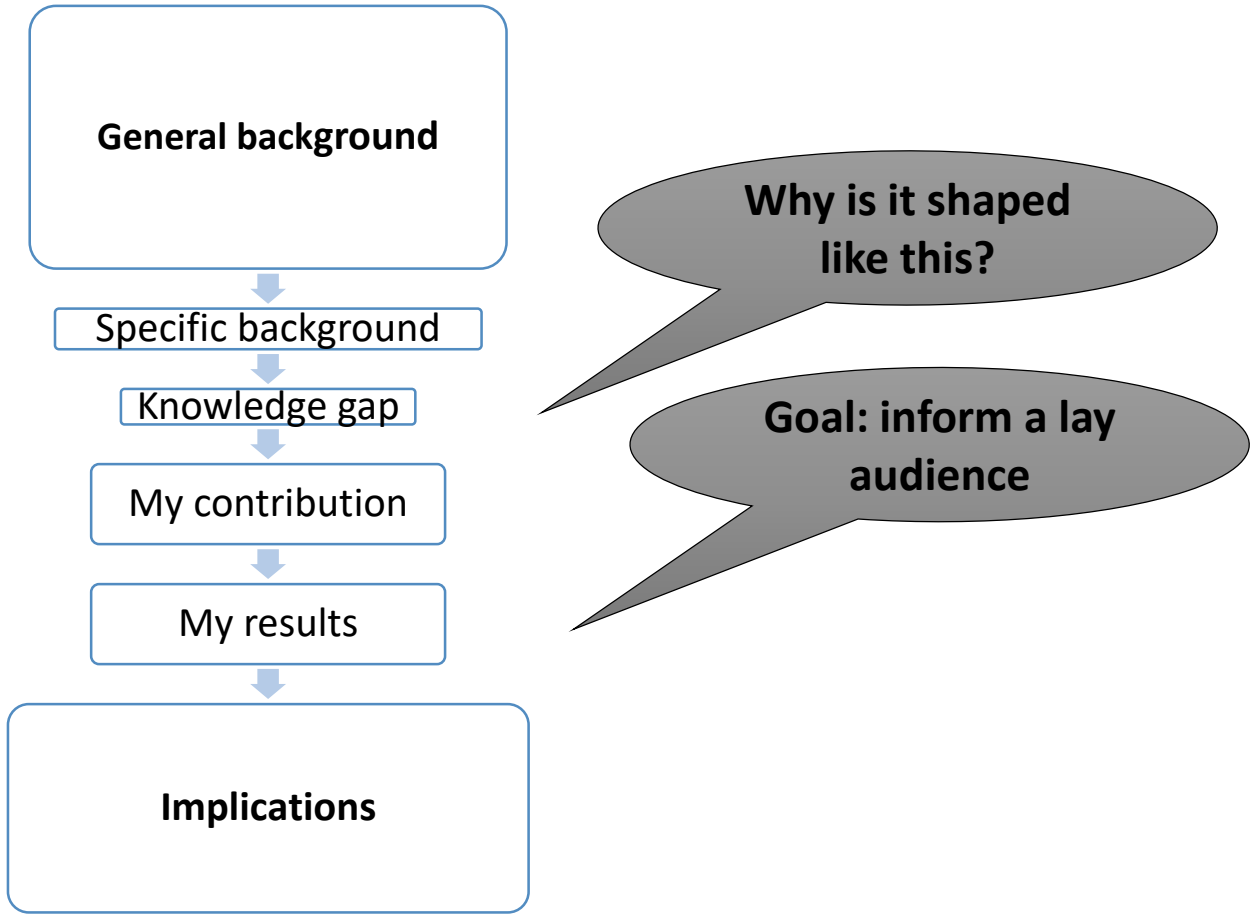
How do I go from this to a lay audience abstract?

An abstract for a general audience is a completely different thing

The heck we are talking about in this workshop

- Goals/emphasis are completely different





When/where would you need a general audience abstract?

- PhD thesis
  - Sometimes universities have a template that requires a non-technical abstract

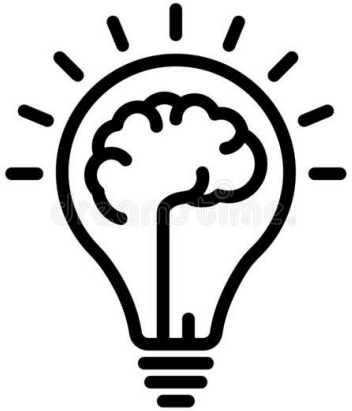
- Project proposal/fellowship
  - The purpose of the abstract is to find reviewers, so it cannot be too technical
  - Abstract will be read by admin person or a panel

- Research popularization/dissemination
  - Newsletter, press release, LinkedIn post

- Webpage description
  - "I do research on ABC for reasons XYZ"

Training?

- Disclaimer: I have **never** received any formal training on this topic
- I have picked up *good habits* from other people
- I have observed *confusion* from PhD students
  - I will show you some examples of what not to do



An example

In the field of my little tiny domain, we have this tiny little problem. In this paper, we are going to talk about things, methods, and approaches that we have put together. It achieves a result like this and like that. This is the best result anyone has ever reported the problem we have studied. Our results are 2.3x better than the best known result reported in the literature.

TAL TECH

An example

In the field of my little tiny domain, we have this tiny little problem. In this paper, we are going to talk about things, methods, and approaches that we have put together. It achieves a result like this and like that. This is the best result anyone has ever reported the problem we have studied. Our results are 2.3x better than the best known result reported in the literature.

How do we go from this…

… to this?

~~In the field of my little tiny domain, we have this tiny little problem. In this paper, we are going to talk about things, methods, and approaches that we have put together. It achieves a result like this and like that. This is the best result anyone has ever reported the problem we have studied. Our results are 2.3x better than the best known result reported in the literature.~~Here is a much better story than whatever rubbish Sam tried to write. Here is a much better story than whatever rubbish Sam tried to write. Here is a much better story than whatever rubbish Sam tried to write. Here is a much better story than whatever rubbish Sam tried to write. Here is a much better story than whatever rubbish Sam tried to write. Here is a much better story than whatever rubbish Sam tried to write.

Two approaches

- Apparently, reading the paper thoroughly is not needed at all

- We will try two different approaches today
- **AP1**: Start from academic abstract and eliminate “issues” one by one
- **AP2**: Rewrite from scratch

- Obviously, AP2 is superior
  - But… **AP1** tells us what to avoid, and that is valuable information
  - But… **AP2** requires a different mindset

AP1: what are the issues?

- Start from academic abstract and eliminate "issues" one by one
  - Acronyms
  - Academic parlance
  - Field-specific jargon
  - Hard concepts

- Here is one example:

In this manuscript, we synthesized an SCA-aware architecture for an AES-capable IC and achieved best-in-class resiliency against information leakage.

TAL TECH

AP1: what are the issues?

- Start from academic abstract and eliminate "issues" one by one
  - **Acronyms**
  - Academic parlance
  - Field-specific jargon
  - Hard concepts

- Here is one example:

*In this manuscript, we synthesized an **SCA**-aware architecture for an **AES**-capable **IC** and achieved best-in-class resiliency against information leakage.*

TAL TECH

AP1: what are the issues?

- Start from academic abstract and eliminate "issues" one by one
  - Acronyms
  - **Academic parlance**
  - Field-specific jargon
  - Hard concepts

- Here is one example:

***In this manuscript**, we synthesized an SCA-aware architecture for an AES-capable IC and achieved **best-in-class** resiliency against information leakage.*

TAL TECH

AP1: what are the issues?

- Start from academic abstract and eliminate "issues" one by one
  - Acronyms
  - Academic parlance
  - **Field-specific jargon**
  - Hard concepts

- Here is one example:

*In this manuscript, we **synthesized** an SCA-aware architecture for an AES-capable **IC** and achieved best-in-class resiliency against information leakage.*

TAL TECH

AP1: what are the issues?

- Start from academic abstract and eliminate "issues" one by one
  - Acronyms
  - Academic parlance
  - Field-specific jargon
  - **Hard concepts**

- Here is one example:

In this work, we synthesized an SCA-aware architecture for an AES-capable IC and achieved best-in-class ***resiliency against information leakage****.*

TAL TECH

Let’s get to work

- On the next slide I will give you an abstract of a real paper
- We are going to dissect it together

- The paper is titled **Design Space Exploration of SABER in 65nm ASIC**

- Notice that even the title already is tough for a lay audience
  - What is a design space exploration?
  - What is SABER?
  - What is 65nm?
  - What is ASIC?

This paper presents a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

TASK 1
2 min
Identify acronyms

You can do it as a group, team, pair…

TAL TECH

*This paper presents a design space exploration for **SABER**, one of the finalists in **NIST**'s quantum-resistant public-key cryptographic standardi[illegible] Our design space exploration targets a 65nm **ASIC** platform and has resu[illegible]on of 6 different architectures. Our exploration is initiated by setti[illegible]ure which is ported from **FPGA**. In order to improve the clock fre[illegible]oal in our exploration), we have employed several optimization[illegible]piled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.*

If you are not an expert, how do you know SABER is not an acronym?

TAL TECH

This paper presents a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

TASK 2
4 min
Identify academic parlance

TAL TECH

This paper presents *a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a* ***baseline architecture*** *which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz w[illegible]n area of 0.314mm^2. Moreover, physical synthesis is carried [illegible]ure and a tapeout-ready layout is presented. The estimated dynamic [illegible] consumption of the high-frequency architecture is approximately 184mW for k[illegible] generation and 187mW for encapsulation or decapsulation operations. These* ***results strongly suggest*** *that our optimized accelerator architecture is* ***well suited*** *for high-speed cryptographic applications.*

This is called hedging

TAL TECH

This paper presents a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

TASK 3

4 min

Identify field-specific jargon (expressions that only a chip designer would use)

TAL TECH

*This paper presents a **design space exploration** for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration **targets a ~~65nm ASIC~~ platform** and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is **ported from FPGA**. In order to **improve the clock frequency** (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, **physical synthesis is carried out** for this architecture and a **tapeout-ready layout** is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.*

TAL TECH

This paper presents a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm^2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

Identify hard concepts

TAL TECH

This paper presents a design space exploration for SABER, one of the finalists in NIST's ***quantum-resistant public-key cryptographic*** *standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architec[illegible], achieves a remarkable clock frequency of 1GHz while only [illegible]ing an area of 0.314mm^2. Moreover, physical synthesis is carried out for th[illegible] architecture and a tapeout-ready layout is presented. The estimated* ***dynamic power consumption*** *of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.*

Could be worse if we had energy instead

Identify hard concepts

TAL TECH

AP1: what are the issues?

- Start from academic abstract and eliminate “issues” one by one
  - Acronyms
  - Academic parlance
  - Field-specific jargon
  - Hard concepts

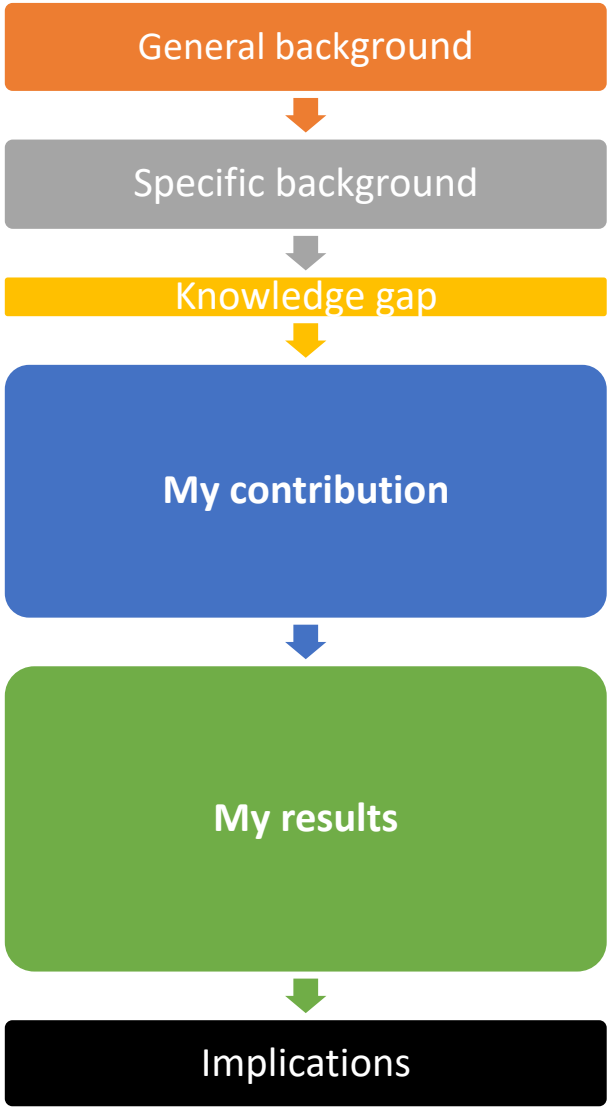
- The key message here is not how to classify the issues
  - There is significant overlap

- The key message is: any term/expression that a lay person will have difficulty understanding should be replaced by a **softer version**

- Now let’s look at **AP2**

TAL TECH

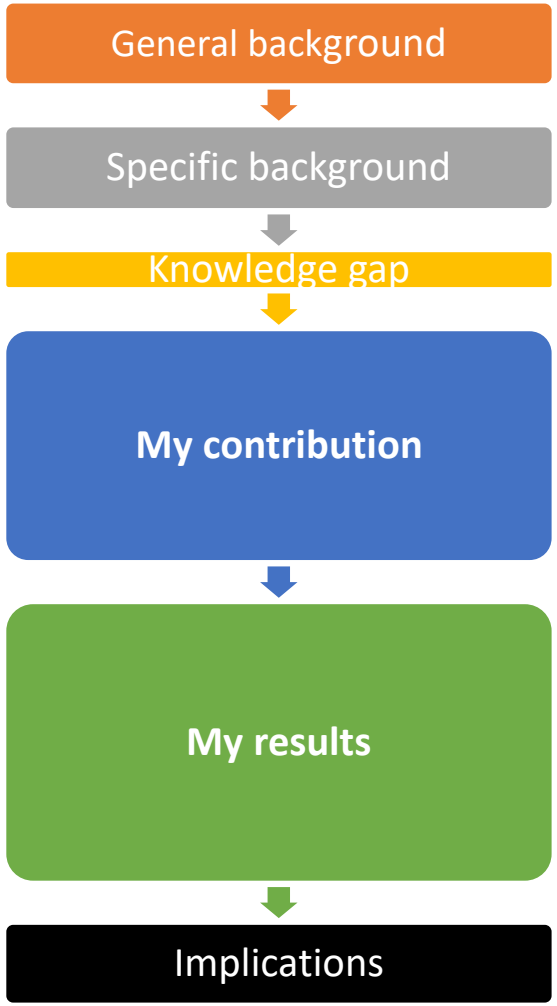
This paper presents a design space exploration for SABER, one of the finalists in NIST's quantum-resistant public-key cryptographic standardization effort. Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations. These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

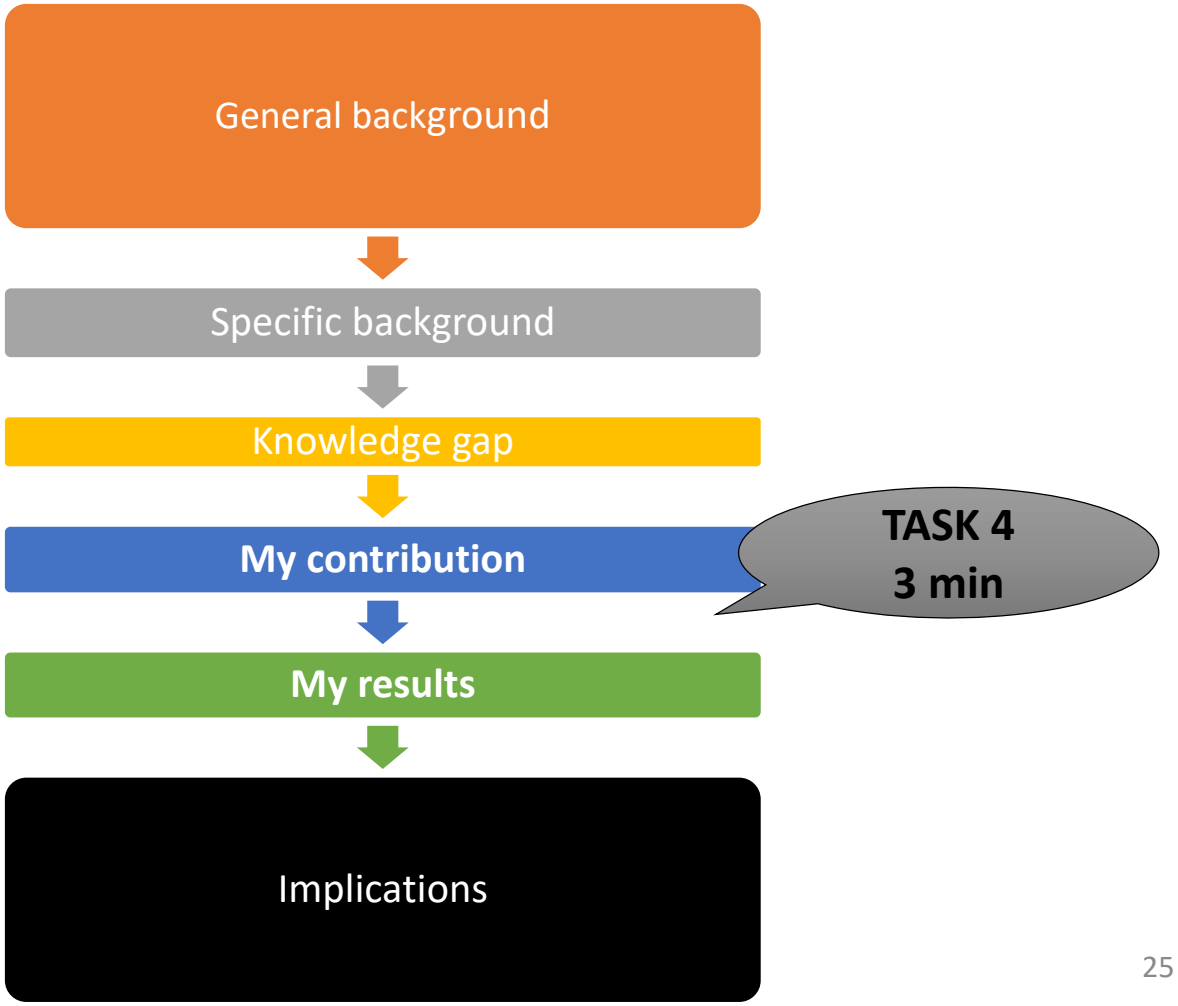


TAL TECH

AP2: writing it from scratch

- Shrink contribution/results to exactly 1 sentence!
  - If it helps, you can write in the third person (The researchers did this… did that…)





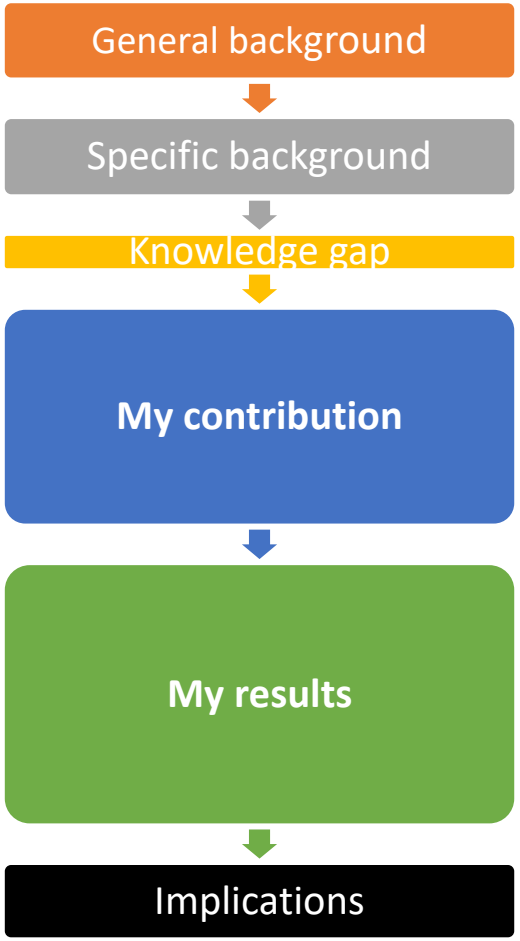
Our design space exploration targets a 65nm ASIC platform and has resulted in the evaluation of 6 different architectures. Our exploration is initiated by setting a baseline architecture which is ported from FPGA. In order to improve the clock frequency (the primary goal in our exploration), we have employed several optimizations: (i) use of compiled memories in a 'smart synthesis' fashion, (ii) pipelining, and (iii) logic sharing between SABER building blocks. The most optimized architecture utilizes four register files, achieves a remarkable clock frequency of 1GHz while only requiring an area of 0.314mm2. Moreover, physical synthesis is carried out for this architecture and a tapeout-ready layout is presented. The estimated dynamic power consumption of the high-frequency architecture is approximately 184mW for key generation and 187mW for encapsulation or decapsulation operations.

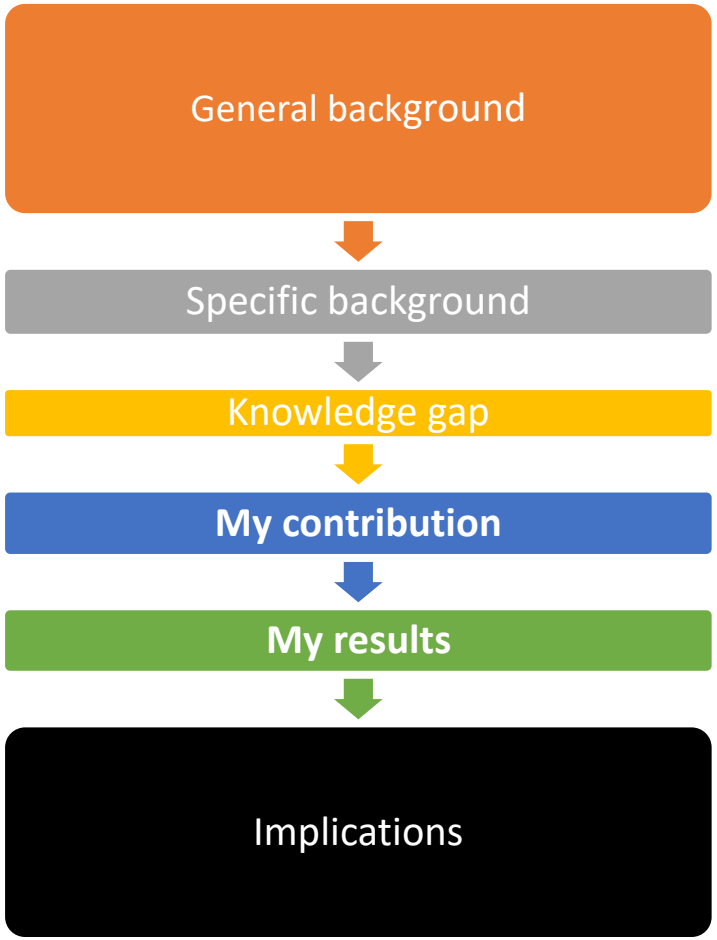
By combining three advanced circuit design techniques, we have achieved a remarkable frequency of 1GHz for our computer chip.

TAL TECH

AP2: writing it from scratch

- Rewrite the implications using 2-3 sentences
  - You must emphasize how the chip is power efficient and how that is good for the planet
  - Green transition, extending battery life, etc.
  - Suggestion: use the angle about logic sharing





TASK 5
5 min

These results strongly suggest that our optimized accelerator architecture is well suited for high-speed cryptographic applications.

In the world of cryptography, algorithms are becoming ever more complicated and power hungry. For this reason, we also made sure that our chip solution is energy efficient by often sharing internal components of the circuit. This means that the chip would help to conserve battery life as much as possible.

TAL TECH

Final remarks

- Writing a lay audience abstract is an important academic skill
  - The Times They Are a-Changin’
  - More and more, researchers are asked to write non-academic text

- General theme
  - Be mindful that your everyday **terms** and **expressions** are very specific
  - Use **softer** ways to explain complex topics
  - Put **emphasis** where emphasis is due

- I hope this was useful to make you think about the problem ☺