Verifying novel cryptography

Forging a forward path

Wrenna Robson

Royal Holloway, University of London

High Integrity Software Conference, 17th October 2023

Table of Contents

1. Overview
   - Novel cryptography
   - Verification
2. The current problem as I see it
   - The state-of-the-art
   - The nature of the problem
3. Details of structured reasoning proposals
4. Wrap-up

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. IT. 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

I intend to circle round these points in a zoomed-out sense, and then in greater details.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

I intend to circle round these points in a zoomed-out sense, and then in greater details. But I'll say, off the bat: I'm sketching a vision, not delivering a solution.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2003

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

I intend to circle round these points in a zoomed-out sense, and then in greater details. But I'll say, off the bat: I'm sketching a vision, not delivering a solution. Overall I am optimistic

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

Verifying novel cryptography: forging a forward path

The aim of this talk is to sketch answers to the following:

- What is novel cryptography, in general and in specific?
- What does it mean to "verify" it?
- What role does verification currently hold in the evaluation of novel cryptography?
- How could this role be improved?

I intend to circle round these points in a zoomed-out sense, and then in greater details. But I'll say, off the bat: I'm sketching a vision, not delivering a solution. Overall I am optimistically pessimistic.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D 2023

What is novel cryptography?

Definition

Novel cryptography refers to a cryptographic system whose design (even if not necessarily the underlying ideas) is newly proposed and to some degree malleable.

What is novel cryptography?

Definition

Novel cryptography refers to a cryptographic system whose design (even if not necessarily the underlying ideas) is newly proposed and to some degree malleable. A cryptosystem ceases to be *novel* in this sense when a version of it is standardised and widely accepted as definitive.

What is novel cryptography?

Definition

Novel cryptography refers to a cryptographic system whose design (even if not necessarily the underlying ideas) is newly proposed and to some degree malleable. A cryptosystem ceases to be *novel* in this sense when a version of it is standardised and widely accepted as definitive. For instance, the Rijndael cryptosystem was once novel cryptography — but once it was standardised as AES it ceased to be so.

What is novel cryptography?

Definition

Novel cryptography refers to a cryptographic system whose design (even if not necessarily the underlying ideas) is newly proposed and to some degree malleable. A cryptosystem ceases to be *novel* in this sense when a version of it is standardised and widely accepted as definitive. For instance, the Rijndael cryptosystem was once novel cryptography — but once it was standardised as AES it ceased to be so.

We make this distinction because, as the design of novel cryptography is by definition malleable, one can meaningfully talk about proposing changes to it based on evaluations of its suitability etc.

What is novel cryptography?

Definition

Novel cryptography refers to a cryptographic system whose design (even if not necessarily the underlying ideas) is newly proposed and to some degree malleable. A cryptosystem ceases to be *novel* in this sense when a version of it is standardised and widely accepted as definitive. For instance, the Rijndael cryptosystem was once novel cryptography — but once it was standardised as AES it ceased to be so.

We make this distinction because, as the design of novel cryptography is by definition malleable, one can meaningfully talk about proposing changes to it based on evaluations of its suitability etc. (It's more than two decades too late to change the fundamental design of AES even if you wanted to.)

Example: NIST Post-Quantum Cryptography Standardization

A relevant example of a source of *novel cryptography* is the NIST Post-Quantum Standardization Process.

Example: NIST Post-Quantum Cryptography Standardization

A relevant example of a source of *novel cryptography* is the NIST Post-Quantum Standardization Process.
To briefly summarise:

- Current public-key cryptography is based on mathematical problems for which efficient quantum algorithms exist.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

Example: NIST Post-Quantum Cryptography Standardization

A relevant example of a source of *novel cryptography* is the NIST Post-Quantum Standardization Process.
To briefly summarise:

- Current public-key cryptography is based on mathematical problems for which efficient quantum algorithms exist.
- A quantum computer might exist in the future, sufficiently soon that many believe we should switch to a new set of standardised algorithms that are resistant to quantum-attack.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Example: NIST Post-Quantum Cryptography Standardization

A relevant example of a source of *novel cryptography* is the NIST Post-Quantum Standardization Process.
To briefly summarise:

- Current public-key cryptography is based on mathematical problems for which efficient quantum algorithms exist.
- A quantum computer might exist in the future, sufficiently soon that many believe we should switch to a new set of standardised algorithms that are resistant to quantum-attack.
- The National Institute of Standards and Technology in the US has been holding an open process for the past 6 or 7 years with the aim of developing, selecting, and standardising a range of suitable candidates.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

Example: NIST Post-Quantum Cryptography Standardization

A relevant example of a source of *novel cryptography* is the NIST Post-Quantum Standardization Process.
To briefly summarise:

- Current public-key cryptography is based on mathematical problems for which efficient quantum algorithms exist.
- A quantum computer might exist in the future, sufficiently soon that many believe we should switch to a new set of standardised algorithms that are resistant to quantum-attack.
- The National Institute of Standards and Technology in the US has been holding an open process for the past 6 or 7 years with the aim of developing, selecting, and standardising a range of suitable candidates.
- The entries for this process constitute novel cryptography: even though some involve old ideas, they are new proposals when taken as a whole.

HISC HIGH INTEGRITY SOFTWARE CONFERENCE EST'D. 2023

State of NIST Post-Quantum Cryptography Standardization

At the current stage in the process, NIST has produced some draft standards, re-opened a call for new proposals on digital signatures, and continues to evaluate some key encapsulation proposals.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. 2023

State of NIST Post-Quantum Cryptography Standardization

At the current stage in the process, NIST has produced some draft standards, re-opened a call for new proposals on digital signatures, and continues to evaluate some key encapsulation proposals.

So the process is highly advanced at this stage, but very much still active.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

State of NIST Post-Quantum Cryptography Standardization

At the current stage in the process, NIST has produced some draft standards, re-opened a call for new proposals on digital signatures, and continues to evaluate some key encapsulation proposals.

So the process is highly advanced at this stage, but very much still active.

Not every example of novel cryptography will be found in a submission to a government agency's standardization efforts... but it is a good example of the sort of thing we mean: and we can definitely ask questions like "is the NIST approach to calling for proposals and evaluating them effective"?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

What is verification?

Definition

The term *verification* and the act of *verifying* is here used in a slightly imprecise sense, to mean any (computer-aided) *production of evidence that a system meets the requirements it is designed to meet*.

Is verification the act of producing such evidence, or is it constructing an argument for the relevance of this evidence?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. IT. 2013

What is verification?

Definition

The term *verification* and the act of *verifying* is here used in a slightly imprecise sense, to mean any (computer-aided) *production of evidence that a system meets the requirements it is designed to meet*.

Is verification the act of producing such evidence, or is it constructing an argument for the relevance of this evidence? We can use it in both ways, which is annoyingly ambiguous, but that's life.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

What is verification?

Definition

The term *verification* and the act of *verifying* is here used in a slightly imprecise sense, to mean any (computer-aided) *production of evidence that a system meets the requirements it is designed to meet*.

Is verification the act of producing such evidence, or is it constructing an argument for the relevance of this evidence? We can use it in both ways, which is annoyingly ambiguous, but that's life. One of the objects of this talk is to tease apart the distinction and to identify the reason the latter happens much less than the former.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

The paradox of computer-aided cryptographu.

There is a healthy community of practitioners of "computer-aided cryptography" — the within-discipline term for "develop[ing] and appl[ying] formal, machine-checkable approaches to the design, analysis, and implementation of cryptography" [BBB+21], which broadly includes what we are calling verification here (and the terms are sometimes imprecisely used synonymously).

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The paradox of computer-aided cryptographu.

There is a healthy community of practitioners of "computer-aided cryptography" — the within-discipline term for "develop[ing] and appl[ying] formal, machine-checkable approaches to the design, analysis, and implementation of cryptography" [BBB+21], which broadly includes what we are calling verification here (and the terms are sometimes imprecisely used synonymously).

Unfortunately, while there is a healthy community of practioners optimistically producing good papers advancing the state-of-the-art in this field, its adoption in industry and especially in wider cryptographic academia is minimal.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The paradox of computer-aided cryptographu.

There is a healthy community of practitioners of "computer-aided cryptography" — the within-discipline term for "develop[ing] and appl[ying] formal, machine-checkable approaches to the design, analysis, and implementation of cryptography" [BBB+21], which broadly includes what we are calling verification here (and the terms are sometimes imprecisely used synonymously).

Unfortunately, while there is a healthy community of practioners optimistically producing good papers advancing the state-of-the-art in this field, its adoption in industry and especially in wider cryptographic academia is minimal.

Not nothing.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

The paradox of computer-aided cryptographu.

There is a healthy community of practitioners of "computer-aided cryptography" — the within-discipline term for "develop[ing] and appl[ying] formal, machine-checkable approaches to the design, analysis, and implementation of cryptography" [BBB+21], which broadly includes what we are calling verification here (and the terms are sometimes imprecisely used synonymously).

Unfortunately, while there is a healthy community of practioners optimistically producing good papers advancing the state-of-the-art in this field, its adoption in industry and especially in wider cryptographic academia is minimal.

Not nothing. But minimal.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

The paradox of computer-aided cryptographu.

There is a healthy community of practitioners of "computer-aided cryptography" — the within-discipline term for "develop[ing] and appl[ying] formal, machine-checkable approaches to the design, analysis, and implementation of cryptography" [BBB+21], which broadly includes what we are calling verification here (and the terms are sometimes imprecisely used synonymously).

Unfortunately, while there is a healthy community of practioners optimistically producing good papers advancing the state-of-the-art in this field, its adoption in industry and especially in wider cryptographic academia is minimal.

Not nothing. But minimal.

I find this paradox very interesting, and one way or another have been picking at it throughout my PhD.

HISC HIGH INTEGRITY SOFTWARE CONFERENCE EST'D. 2023

The state-of-the-art: overview

I would say the absolute state-of-the-art in verifying novel cryptography — indeed, in producing high-assurance cryptography of any kind — is found in a recent paper from TCHES. [BABB+23]

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. 2023

The state-of-the-art: overview

I would say the absolute state-of-the-art in verifying novel cryptography — indeed, in producing high-assurance cryptography of any kind — is found in a recent paper from TCHES. [BABB+23] This paper presents an end-to-end verification of Kyber, the only KEM selected so far for standardization by NIST.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The state-of-the-art: overview

I would say the absolute state-of-the-art in verifying novel cryptography — indeed, in producing high-assurance cryptography of any kind — is found in a recent paper from TCHES. [BABB+23] This paper presents an end-to-end verification of Kyber, the only KEM selected so far for standardization by NIST. It presents a formalisation of the Kyber specification, an implementation of Kyber in Jasmin, a language purpose-built for high-speed, high-assurance cryptography, an extraction of a model from this implementation into EasyCrypt, a tool built for verification of security proofs, and the necessary proofs required to show that these are all compatible with one another.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The state-of-the-art: overview

I would say the absolute state-of-the-art in verifying novel cryptography — indeed, in producing high-assurance cryptography of any kind — is found in a recent paper from TCHES. [BABB+23] This paper presents an end-to-end verification of Kyber, the only KEM selected so far for standardization by NIST. It presents a formalisation of the Kyber specification, an implementation of Kyber in Jasmin, a language purpose-built for high-speed, high-assurance cryptography, an extraction of a model from this implementation into EasyCrypt, a tool built for verification of security proofs, and the necessary proofs required to show that these are all compatible with one another.

And the implementation is performant. It's a tremendous achievement, in my view.

The state-of-the-art: overview

I would say the absolute state-of-the-art in verifying novel cryptography — indeed, in producing high-assurance cryptography of any kind — is found in a recent paper from TCHES. [BABB+23] This paper presents an end-to-end verification of Kyber, the only KEM selected so far for standardization by NIST. It presents a formalisation of the Kyber specification, an implementation of Kyber in Jasmin, a language purpose-built for high-speed, high-assurance cryptography, an extraction of a model from this implementation into EasyCrypt, a tool built for verification of security proofs, and the necessary proofs required to show that these are all compatible with one another.

And the implementation is performant. It's a tremendous achievement, in my view. It also took nearly three years of work from more experts in the field than I can count on one hand and perhaps on two. They make a very persuasive case for the value of their work, but undoubtedly it has great costs in time and resources.

The state-of-the-art: assurance case

Ultimately, this work presents a host of verification artifacts — great chunks of it are "self-justifying", even, in the sense that they prove things about their own constructions.

The state-of-the-art: assurance case

Ultimately, this work presents a host of verification artifacts — great chunks of it are "self-justifying", even, in the sense that they prove things about their own constructions. It is rational to believe their implementation is functionally correct, and obeys the security properties as they have modelled them.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The state-of-the-art: assurance case

Ultimately, this work presents a host of verification artifacts — great chunks of it are "self-justifying", even, in the sense that they prove things about their own constructions. It is rational to believe their implementation is functionally correct, and obeys the security properties as they have modelled them.

But what does this mean? What should we take from this? The authors make no major attempt at linking any of their efforts to an assurance case for Kyber, or to Kyber's specific design to the extent it can now be changed.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The state-of-the-art: assurance case

Ultimately, this work presents a host of verification artifacts — great chunks of it are "self-justifying", even, in the sense that they prove things about their own constructions. It is rational to believe their implementation is functionally correct, and obeys the security properties as they have modelled them.

But what does this mean? What should we take from this? The authors make no major attempt at linking any of their efforts to an assurance case for Kyber, or to Kyber's specific design to the extent it can now be changed.

Does this tell us *anything* about the implementations of Kyber that will actually be deployed in practice?

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

Street cryptography

What does any of this mean to the cryptographer “on the street”?

Street cryptography

What does any of this mean to the cryptographer "on the street"?
There were a score or more submissions to the original NIST call for proposals. There are many more which have been submitted to their new call for signature schemes.

Street cryptography

What does any of this mean to the cryptographer "on the street"?
There were a score or more submissions to the original NIST call for proposals. There are many more which have been submitted to their new call for signature schemes.

Nearly none of them make any attempt to use automated verification as part of the case for their scheme. Indeed, in many cases, even in the submission documents, the details of the assurance case for the submission is murky. It certainly isn't clear how the evidence from verification would fit in.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Street cryptography

What does any of this mean to the cryptographer "on the street"?
There were a score or more submissions to the original NIST call for proposals. There are many more which have been submitted to their new call for signature schemes.

Nearly none of them make any attempt to use automated verification as part of the case for their scheme. Indeed, in many cases, even in the submission documents, the details of the assurance case for the submission is murky. It certainly isn't clear how the evidence from verification would fit in. Clearly it is possible to evaluate these submissions. NIST have done so, painstakingly.
But I think better is possible, and desirable.

Observations of the “pqc-forum” mailing list

I have been a keen reader of the “pqc-forum” mailing list, administered by NIST, which is essentially the central location for public discussion of the NIST submissions.

Observations of the “pqc-forum” mailing list

I have been a keen reader of the “pqc-forum” mailing list, administered by NIST, which is essentially the central location for public discussion of the NIST submissions. Putting aside the small amount of spam messages, this is generally a great place to see what actually matters to the cryptographers working on this technology: what is discussed, what isn't, what provokes heated discussion and what does not.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Observations of the “pqc-forum” mailing list

I have been a keen reader of the “pqc-forum” mailing list, administered by NIST, which is essentially the central location for public discussion of the NIST submissions. Putting aside the small amount of spam messages, this is generally a great place to see what actually matters to the cryptographers working on this technology: what is discussed, what isn't, what provokes heated discussion and what does not.

What I would say is that the more heated discussions here are often about the details of what statements mean, and whether they are validly interpreted. It seems to be the thing that trips people up the most.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Observations of the “pqc-forum” mailing list

I have been a keen reader of the “pqc-forum” mailing list, administered by NIST, which is essentially the central location for public discussion of the NIST submissions. Putting aside the small amount of spam messages, this is generally a great place to see what actually matters to the cryptographers working on this technology: what is discussed, what isn't, what provokes heated discussion and what does not.

What I would say is that the more heated discussions here are often about the details of what statements mean, and whether they are validly interpreted. It seems to be the thing that trips people up the most. Arguments for or against a particular proposal, attacks on or refutation of attacks on those proposals: these are common. As the participants in these discussions are experts working at a high-level in this topic, the reasoning chains for particular claims sometimes remain implicit.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Observations of the “pqc-forum” mailing list

I have been a keen reader of the “pqc-forum” mailing list, administered by NIST, which is essentially the central location for public discussion of the NIST submissions. Putting aside the small amount of spam messages, this is generally a great place to see what actually matters to the cryptographers working on this technology: what is discussed, what isn't, what provokes heated discussion and what does not.

What I would say is that the more heated discussions here are often about the details of what statements mean, and whether they are validly interpreted. It seems to be the thing that trips people up the most. Arguments for or against a particular proposal, attacks on or refutation of attacks on those proposals: these are common. As the participants in these discussions are experts working at a high-level in this topic, the reasoning chains for particular claims sometimes remain implicit.

This extends even to the draft standards themselves.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

Structural change

I claim: a structural change in how we reason about and evaluate novel cryptography is highly desirable. By 'a structural change', I mean a change to how the reasoning is presented and conceived.

Structural change

I claim: a structural change in how we reason about and evaluate novel cryptography is highly desirable. By 'a structural change', I mean a change to how the reasoning is presented and conceived.

By reason about, I mean: we want the claims of provable security to be meaningful.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D 2003

Structural change

I claim: a structural change in how we reason about and evaluate novel cryptography is highly desirable. By 'a structural change', I mean a change to how the reasoning is presented and conceived.

By reason about, I mean: we want the claims of provable security to be meaningful.

By evaluate, I am talking about, for example, the way that submissions to the NIST process are evaluated against the 'Call for Proposals'. If one is going to pose a requirements document that some novel cryptography must meet, then the submission must include a clear explanation of how each required criteria is addressed, in a structured way that leaves no room for ambiguity.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

Seeing things as an assurance case

In essense: what I am arguing is that a case for a particular design or implementation of novel cryptography is an assurance case — "this design is secure", "this implementation is right".

Seeing things as an assurance case

In essense: what I am arguing is that a case for a particular design or implementation of novel cryptography is an assurance case — "this design is secure", "this implementation is right".

So: let us not start from scratch. There is a whole discipline about how to write a good assurance case, whole conferences, like this one, about how to create and use high-integrity software.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Seeing things as an assurance case

In essense: what I am arguing is that a case for a particular design or implementation of novel cryptography is an assurance case — "this design is secure", "this implementation is right".

So: let us not start from scratch. There is a whole discipline about how to write a good assurance case, whole conferences, like this one, about how to create and use high-integrity software. Essentially, the advantage to framing this as a formal assurance case is that we can then benefit from the fact that people have already spent a large amount of time thinking about what a good case looks like.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2003

Seeing things as an assurance case

In essense: what I am arguing is that a case for a particular design or implementation of novel cryptography is an assurance case — "this design is secure", "this implementation is right".

So: let us not start from scratch. There is a whole discipline about how to write a good assurance case, whole conferences, like this one, about how to create and use high-integrity software. Essentially, the advantage to framing this as a formal assurance case is that we can then benefit from the fact that people have already spent a large amount of time thinking about what a good case looks like.

In particular, if you have a structured reasoning framework, it is a lot easier to work out how to integrate the results of formal verification into this framework. Without it, it can be nebulous — too often, I see people gesture towards the idea of formal proof with no indication as to what it supports, or what meaning it should have in context.

Bridging worlds

We have the cryptography world, and we have the high-integrity software world. It is desirable in and of itself to bridge the two, but also it has the advantage of making it easier to connect the former to the 'computer-aided cryptography/formal verification' world. These worlds, empirically, are not currently that strongly linked in terms of the work of the latter finding practical use.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

Bridging worlds

We have the cryptography world, and we have the high-integrity software world. It is desirable in and of itself to bridge the two, but also it has the advantage of making it easier to connect the former to the 'computer-aided cryptography/formal verification' world. These worlds, empirically, are not currently that strongly linked in terms of the work of the latter finding practical use.

To reiterate: empirically just means 'looking at the revealed preferences derived from people's behaviour'.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

The meaning of formal verification

I think it is hard to explain what a verification actually means.

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

What is the meaning of any proof?

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

What is the meaning of any proof? The meaning of a pen-and-paper proof is not 'what is written in the theorem statement'. Indeed, it's well-known that even with pen-and-paper, the method of proof can contain insight into the structure of the objects being reasoned about.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

What is the meaning of any proof? The meaning of a pen-and-paper proof is not 'what is written in the theorem statement'. Indeed, it's well-known that even with pen-and-paper, the method of proof can contain insight into the structure of the objects being reasoned about. THe meaning of a pen-and-paper proof derives from it being read and understood, and integrated into a wider understanding.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

What is the meaning of any proof? The meaning of a pen-and-paper proof is not 'what is written in the theorem statement'. Indeed, it's well-known that even with pen-and-paper, the method of proof can contain insight into the structure of the objects being reasoned about. THe meaning of a pen-and-paper proof derives from it being read and understood, and integrated into a wider understanding. What makes a valid proof? It depends who's asking.

The meaning of formal verification

I think it is hard to explain what a verification actually means. This is a subtle point, I think.

What is the meaning of any proof? The meaning of a pen-and-paper proof is not 'what is written in the theorem statement'. Indeed, it's well-known that even with pen-and-paper, the method of proof can contain insight into the structure of the objects being reasoned about. THe meaning of a pen-and-paper proof derives from it being read and understood, and integrated into a wider understanding. What makes a valid proof? It depends who's asking.

The observation I make is that this is no less true of formal verification. If a formal proof is to be regarded as a form of evidence for the security of an implementation or design, that evidence has meaning only alongside the claims it justifies and the argument which links them to a web of justified belief.

HISC HIGH INTEGRITY SOFTWARE CONFERENCE EST'D 2023

Claims, argument, evidence: a reasoning framework

After some time thinking about this problem — in the context of trying different methods of formal verification on a particular post-quantum proposal in order to evaluate the merits of various approaches — I came to the Claims, Argument, Evidence reasoning and communication framework pioneered by Adelard, now part of the NCC group.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Claims, argument, evidence: a reasoning framework

After some time thinking about this problem — in the context of trying different methods of formal verification on a particular post-quantum proposal in order to evaluate the merits of various approaches — I came to the Claims, Argument, Evidence reasoning and communication framework pioneered by Adelard, now part of the NCC group.

Verification artifacts are often presented as both evidence and argument. However, often, the actual explanation of the link between "this verification has been performed" and a particular claim is missing or obscured.

Claims, argument, evidence: a reasoning framework

After some time thinking about this problem — in the context of trying different methods of formal verification on a particular post-quantum proposal in order to evaluate the merits of various approaches — I came to the Claims, Argument, Evidence reasoning and communication framework pioneered by Adelard, now part of the NCC group.

Verification artifacts are often presented as both evidence and argument. However, often, the actual explanation of the link between "this verification has been performed" and a particular claim is missing or obscured. It isn't unheard of to see a talismanic approach to verification — "oh, we should do some formal verification here, that will increase confidence in the scheme" — with no explanation as to how or why this will occur.

HISC HIGH INTEGRITY SOFTWARE CONFERENCE EST'D. 2023

Dangling assurance cases

I argue that what is really happening when a body like NIST puts forth a call for proposals — whenever there is a provocation towards cryptographic innovation — is that a "dangling assurance case" is being created.

Dangling assurance cases

I argue that what is really happening when a body like NIST puts forth a call for proposals — whenever there is a provocation towards cryptographic innovation — is that a "dangling assurance case" is being created.

It isn't quite correct to call this a specification — or if it is one, it is a very general specification. What is present is a host of unjustified claims and unresolved defeaters, to use the language of Assurance 2.0 [BR23].

Dangling assurance cases

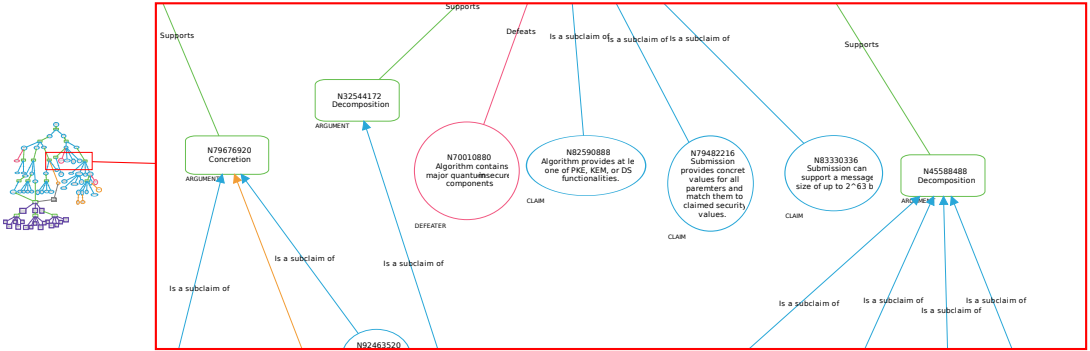
I argue that what is really happening when a body like NIST puts forth a call for proposals — whenever there is a provocation towards cryptographic innovation — is that a "dangling assurance case" is being created.

It isn't quite correct to call this a specification — or if it is one, it is a very general specification. What is present is a host of unjustified claims and unresolved defeaters, to use the language of Assurance 2.0 [BR23].

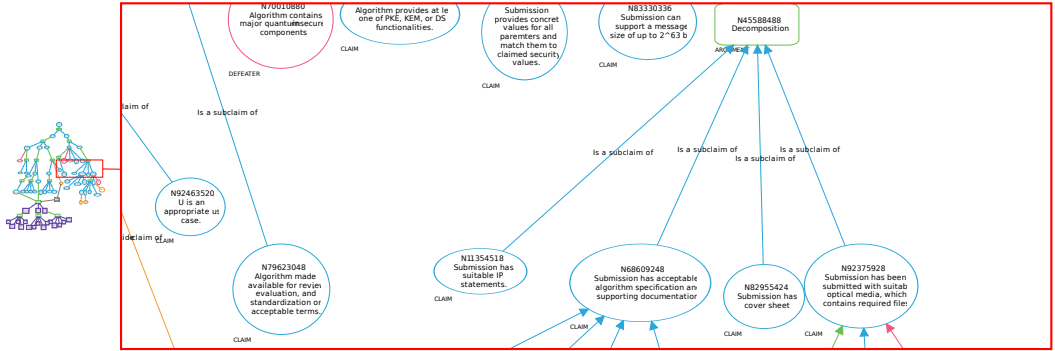
The case for a particular piece of novel cryptography is an answer to this dangling case — an assertion that there is a specific fufillment of the problem it poses. In this perspective, a good scheme is precisely one which wholly justifies its fufillment of unjustified claims, and resolves satisfactorily any potential defeaters.

HISC HIGH INTEGRITY SOFTWARE CONFERENCE EST'D. 2023

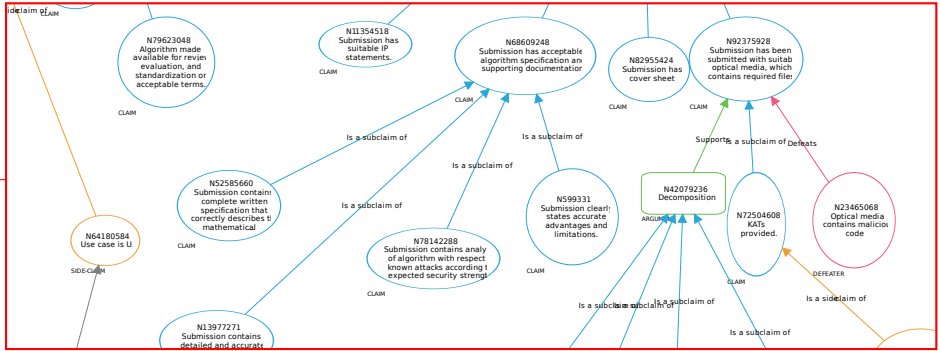
Example: Analysing the NIST Call for Proposals



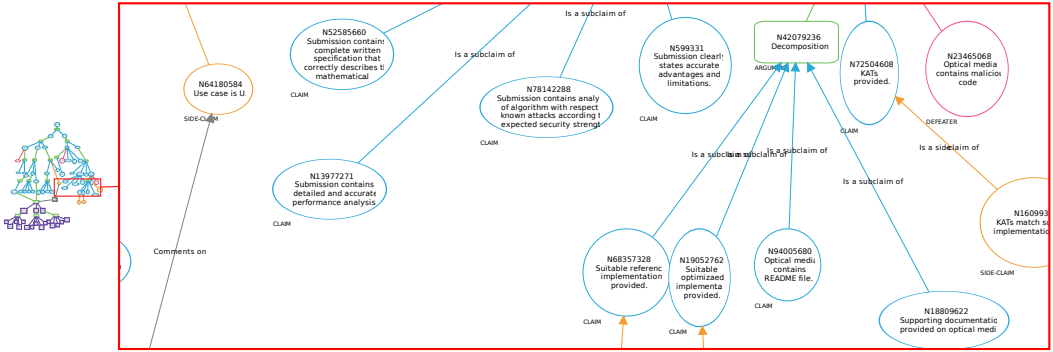
Example: Analysing the NIST Call for Proposals



Example: Analysing the NIST Call for Proposals

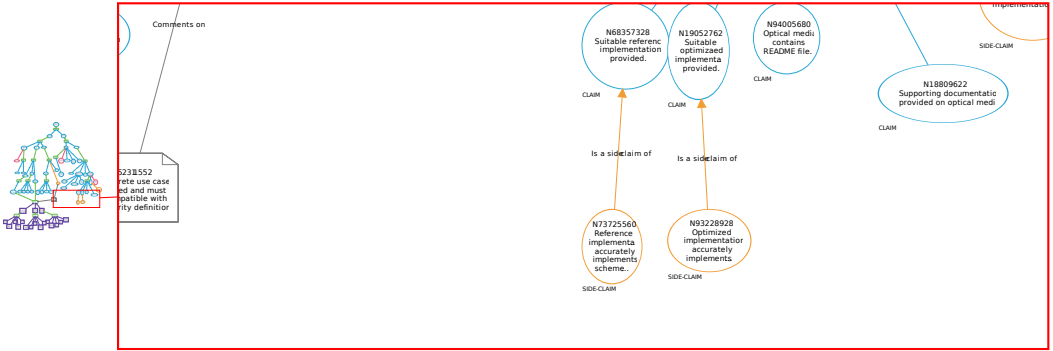


Example: Analysing the NIST Call for Proposals

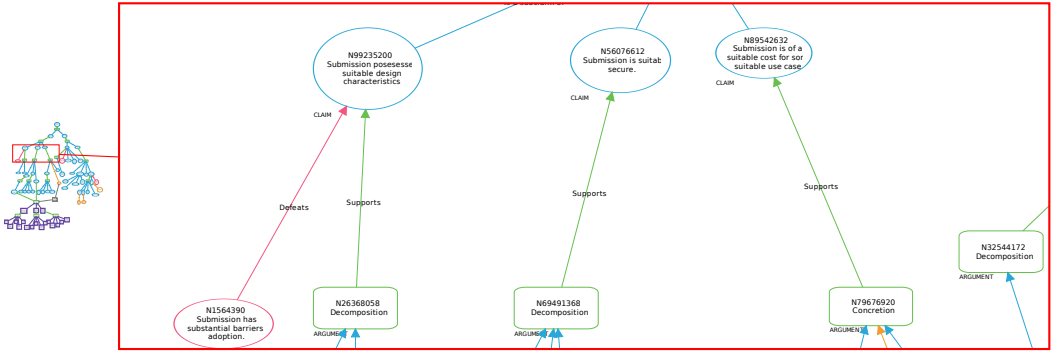


HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 17, 2023

Example: Analysing the NIST Call for Proposals

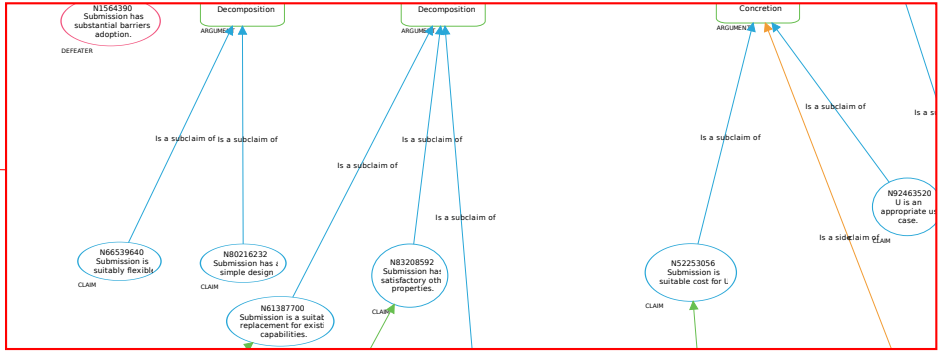


Example: Analysing the NIST Call for Proposals

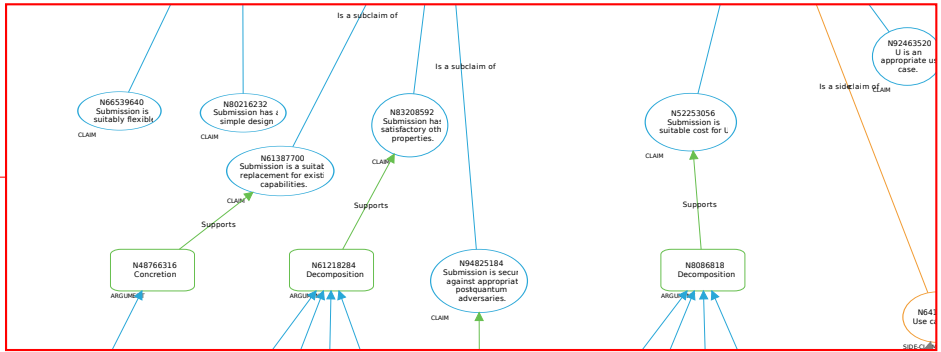


HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. 2023

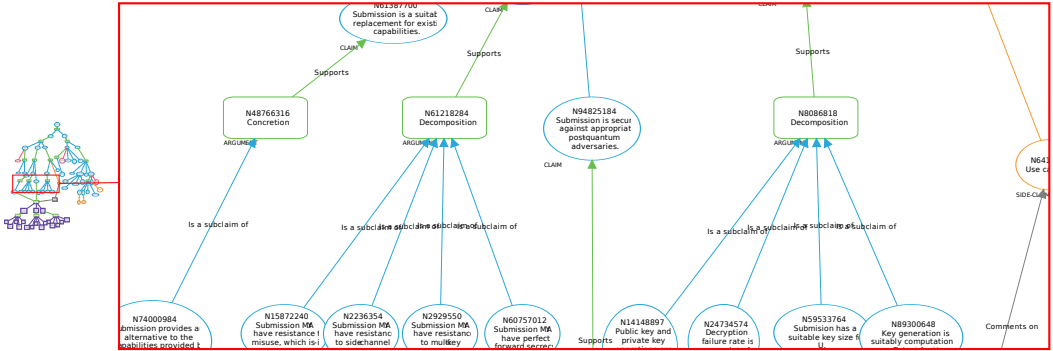
Example: Analysing the NIST Call for Proposals



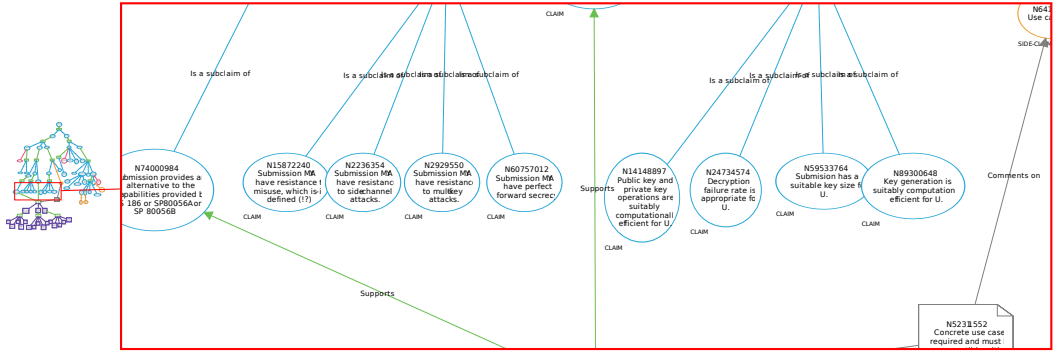
Example: Analysing the NIST Call for Proposals



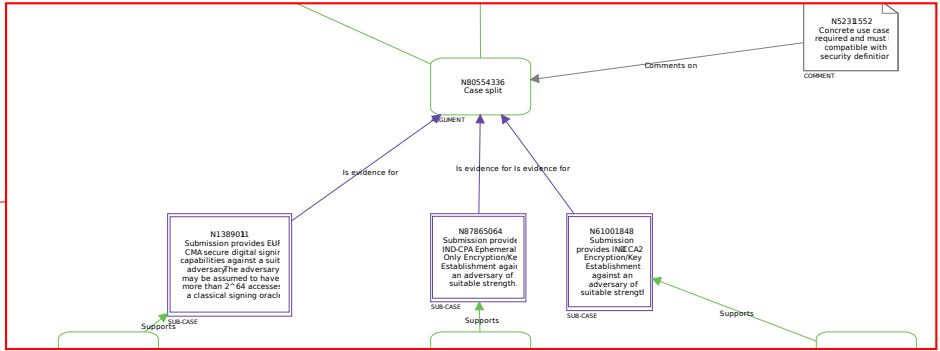
Example: Analysing the NIST Call for Proposals



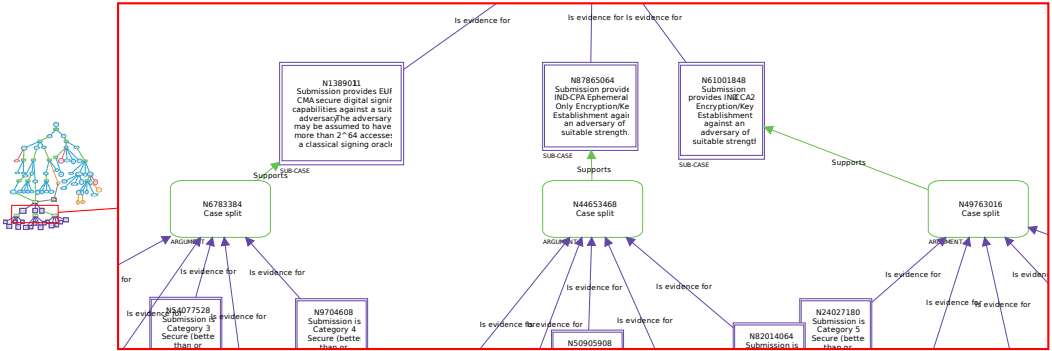
Example: Analysing the NIST Call for Proposals



Example: Analysing the NIST Call for Proposals



Example: Analysing the NIST Call for Proposals



Who is responsible?

Essentially this is a sketch of a way forward.

Who is responsible?

Essentially this is a sketch of a way forward. The current way of doing things is fine.

Who is responsible?

Essentially this is a sketch of a way forward. The current way of doing things is fine. As I say, I think better is possible: asking for argumentation and evidence in a more structured, standardised form could engender a new approach.

Who is responsible?

Essentially this is a sketch of a way forward. The current way of doing things is fine. As I say, I think better is possible: asking for argumentation and evidence in a more structured, standardised form could engender a new approach.

Who is to do this? In a sense it will only happen if standards bodies, government agencies etc. are interested in such an approach.

Who is responsible?

Essentially this is a sketch of a way forward. The current way of doing things is fine. As I say, I think better is possible: asking for argumentation and evidence in a more structured, standardised form could engender a new approach.

Who is to do this? In a sense it will only happen if standards bodies, government agencies etc. are interested in such an approach. I believe the NCSC in the UK is pursuing the promotion of what it calls Principles Based Assurance. This seems to me to be interesting and useful. I don't know to what degree it would be adapatable for these purposes! But I am intrigued.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2003

Who is responsible?

Essentially this is a sketch of a way forward. The current way of doing things is fine. As I say, I think better is possible: asking for argumentation and evidence in a more structured, standardised form could engender a new approach.

Who is to do this? In a sense it will only happen if standards bodies, government agencies etc. are interested in such an approach. I believe the NCSC in the UK is pursuing the promotion of what it calls Principles Based Assurance. This seems to me to be interesting and useful. I don't know to what degree it would be adapatable for these purposes! But I am intrigued.

I argue "If you build it, they will come" — if the expectations and standards are clear, then people will adapt to them. I think a rules-based, principle-based, evidence-based approach to novel cryptography assurance cases is sensible and possible — but someone needs to light the way.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D. 2023

CAE Tooling & Thoughts

I have used Adelard's ACSE a little. Seems good — but I note that academics are often resistant to the use of proprietary software — and academics are often the people creating novel cryptography.

CAE Tooling & Thoughts

I have used Adelard's ACSE a little. Seems good — but I note that academics are often resistant to the use of proprietary software — and academics are often the people creating novel cryptography. There are other tools out there for other forms of Goal-Structuring Notation. Which ones are good? Which ones are actually reasonable to ask people to adopt?

CAE Tooling & Thoughts

I have used Adelard's ACSE a little. Seems good — but I note that academics are often resistant to the use of proprietary software — and academics are often the people creating novel cryptography. There are other tools out there for other forms of Goal-Structuring Notation. Which ones are good? Which ones are actually reasonable to ask people to adopt?

Security arguments in cryptography often use arguments of the form 'P. If not-Q then not-P. Thus, Q.' (The so-called proof by contrapositive.)

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

CAE Tooling & Thoughts

I have used Adelard's ACSE a little. Seems good — but I note that academics are often resistant to the use of proprietary software — and academics are often the people creating novel cryptography. There are other tools out there for other forms of Goal-Structuring Notation. Which ones are good? Which ones are actually reasonable to ask people to adopt?

Security arguments in cryptography often use arguments of the form 'P. If not-Q then not-P. Thus, Q.' (The so-called proof by contrapositive.) This argument is often fairly non-constructive in its form: secretly it uses, I think, the law of the excluded middle.

A little about me

Just to give you some context about where I'm coming from in all this:

A little about me

Just to give you some context about where I'm coming from in all this: I'm near the end of a PhD at Royal Holloway's Centre for Cyber Security in the Everyday. I have two supervisors: Dr Rachel Player within the college handles the cryptography end of things, and Dr Martin Brain of City University has been my route into the verification community.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

A little about me

Just to give you some context about where I'm coming from in all this: I'm near the end of a PhD at Royal Holloway's Centre for Cyber Security in the Everyday. I have two supervisors: Dr Rachel Player within the college handles the cryptography end of things, and Dr Martin Brain of City University has been my route into the verification community.

I've spent my PhD approaching the verification of different aspects (mainly functional correctness) of Classic McEliece with different tools. I'm now writing up case studies and drawing conclusions into my thesis, which was the motivation of the thought that sparked this talk.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST IT. 2023

The future

I'm considering submitting something on this to the upcoming NIST conference if I can get my thoughts together in time. I'm interested to hear more about any prior work which anyone is aware of using CAE arguments in a cryptographic context.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST'D 2023

The future

I'm considering submitting something on this to the upcoming NIST conference if I can get my thoughts together in time. I'm interested to hear more about any prior work which anyone is aware of using CAE arguments in a cryptographic context.

I should be finishing my PhD in Spring 2024, and I'm looking for work in this area in academia or industry.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
EST. IT. 2023

The future

I'm considering submitting something on this to the upcoming NIST conference if I can get my thoughts together in time. I'm interested to hear more about any prior work which anyone is aware of using CAE arguments in a cryptographic context.

I should be finishing my PhD in Spring 2024, and I'm looking for work in this area in academia or industry.

I can be contacted on `wren.robson@gmail.com` if you have further comment on anything I've talked about today.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 11, 2023

Bibliography

José Bacelar Almeida, Manuel Barbosa, Gilles Barthe, Benjamin Grégoire, Vincent Laporte, Jean-Christophe Léchenet, Tiago Oliveira, Hugo Pacheco, Miguel Quaresma, Peter Schwabe, and et al.
Formally verifying kyber: Episode iv: Implementation correctness.
IACR Transactions on Cryptographic Hardware and Embedded Systems, 2023(3):164–193, Jun. 2023.

Manuel Barbosa, Gilles Barthe, Karthik Bhargavan, Bruno Blanchet, Cas Cremers, Kevin Liao, and Bryan Parno.
SoK: Computer-aided cryptography.
In *2021 IEEE Symposium on Security and Privacy (SP)*, pages 777–795. IEEE, 2021.

Robin Bloomfield and John Rushby.
Assessing confidence with assurance 2.0, 2023.

HISC
HIGH INTEGRITY SOFTWARE CONFERENCE
OCT 31, 2023