

Cryptol: A Domain Specific Language for Verification of Cryptographic Algorithms

Zhiyuan Lin

July 25, 2016

Abstract

Implementing reliable cryptographic protocols is a difficult task, and the Cryptol language is an attempt at using programming language to improve reliability of cryptographic implementations. The language provides interesting features such as a powerful type system, and native support for formal verification. In this study we evaluate Cryptol through the combination of a literature survey and an implementation project. We conclude that Cryptol language is well suited for cryptography, although it still has a long way to go to become a practical language.

Contents

1	Introduction	3
2	Literature Survey	5
2.1	The Cryptol Language	5
2.1.1	The Standard Language of Cryptography	6
2.1.2	High Assurance Programming	6
2.1.3	How Formal Verification Works in Cryptol	8
2.2	Languages for Cryptographic Applications	9
3	Implementation and Evaluation	11
3.1	The AES Algorithm	11
3.2	Implementation Details	13
3.3	Implementation and Verification	13
3.4	Review of the Cryptol Language	15
4	Conclusion and Future Works	19

Chapter 1

Introduction

Cryptographic protocols are used everywhere nowadays. Google, for example, recently claimed in its transparency report that 75% of the requests to its servers are now encrypted. However, providing secure implementations of cryptographic algorithms remains a difficult task, even for experienced security engineers and researchers. Cryptographic algorithms often involve a lot of advanced number theory. Without a proper understanding of the background theory it is difficult to implement protocols with the necessary level of precision and precaution. Simple mistakes such as failing to validate input, or reusing keys could compromise the security of the entire system. Moreover, recent cryptographic algorithms are often only specified in academic publications, which by nature focus on the background theory and security proofs of the protocols, instead of implementation details. Even if the protocol follows the specification, the system must still be secured against side-channel attacks. There are also human factors that might affect security of cryptographic protocols. An secure protocol when used improperly could also result in leakage of information. With all these potential issues to be resolved, it is no wonder why many existing implementations of cryptographic protocols have or had known vulnerabilities. OpenSSL, one of the most widely-used implementation of SSL and TLS protocols, still suffer from constant criticism and had famous bugs such as Heartbleed.

There have been many studies on improving the reliability of cryptographic implementations. Some try to tackle the problem from a programming language perspective. These studies propose that instead of using traditional languages such as C and C++, which offers little guarantees to the program, we should create high-level, performant programming languages that are dedicated to the subject of cryptography. Among these attempts, the Cryptol programming language is a good example with a unique combination of features.

Cryptol is a pure functional programming language with native support for formal verification, and it is designed specifically to be the language of cryptography. With these unique features, it would be interesting to see if the

language delivers on its promises. That is exactly the purpose of this project: to investigate and evaluate the Cryptol programming language. This study provides insight on whether new programming languages can serve as useful tools for enhancing cryptographic implementation, and what language features are important for cryptography. We discuss our approach and contributions below.

Organization and Contributions

This project involves two major components. The first part of the project is a literature survey, presented in Chapter 2. We introduce the essential features such as the type system of the Cryptol language and the theory behind its formal verification utilities in this chapter. Furthermore, we cover other domain specific languages and related tools for cryptography extensively and compare these languages with Cryptol. This part of the project not only serves as the foundation for further discussion, but also gives an overview of the field of languages for cryptography.

In the section part of the project, we evaluate the Cryptol programming language by implementing and verifying the AES algorithm. This includes implementing the algorithm in a functional style, and devising properties that can be proved for the implementation. We also summarize the experience of using Cryptol and provide constructive feedback on the features of Cryptol. Combined with the survey, this gives us a comprehensive evaluation of the Cryptol language. This part of the results are discussed in Chapter 3.

Finally in Chapter 4 we summarize the study and discuss ideas for future developments.

Chapter 2

Literature Survey

In this chapter we present previous researches that use programming language as a means to improve reliability of cryptographic applications.

We start with a detailed introduction to the essential features and design objectives of the Cryptol language in Section 2.1, followed by a comprehensive survey of related works that use programming language to improve reliability of cryptographic implementation in Section 2.2.

2.1 The Cryptol Language

As has been mentioned before, Cryptol is a high-level programming language designed for cryptography. It provides a formal methods-based approach to cryptographic developments.

The Cryptol language is designed with several objectives in mind:

- Cryptol is designed to be the standard language of cryptography
- The Cryptol language provides high assurance of the correctness of the implementation
- The Cryptol source program can be used as source for code generation to multiple target platforms

We introduce the features that bring about these benefits in detail below.

1	<code>encrypt: {n} (0 < n, n < 3) => [8*n] -> [8*n]</code>
---	--

Figure 2.1: Cryptol Type Signature

2.1.1 The Standard Language of Cryptography

Cryptol is ambitiously designed to become the standard language of cryptography. Implementation of cryptographic algorithms in Cryptol are expected to serve as a high-level formal specification or at least reference implementation of the algorithms. This means that the language allows for algorithms specified in academic papers and standards to be translated into Cryptol source code in a manner that is straightforward and readable. Moreover, Cryptol frees developers from machine level details so that they could focus on developing new algorithms.

To achieve this goal, Cryptol is designed to be a pure functional programming language similar to Haskell. The Cryptol syntax, just like Haskell's, is heavily inspired by mathematical notations, and therefore can express computations in cryptographic protocols easily. It is also argued that functional programs are usually shorter and easier to understand. The persistent data structures provided in Cryptol allows for easier analysis and optimization of computation. Furthermore, the functional style naturally helps to create simple and clean abstractions so that the program is well-structured.

2.1.2 High Assurance Programming

To serve as authoritative specifications, Cryptol programs need to be correct first. Cryptol comes with several features that provide strong guarantee of the correctness of functions:

- Type System
- Formal Verification
- Automated Testing

Type System

Cryptol uses a type system based on the Hindley-Milner type system [16], extend with size-polymorphism and arithmetic type predicates [3]. The type system is designed to capture constraints that naturally arise from cryptographic algorithms such as fixed-size keys and input blocks.

See Figure 2.1 for an example of type signatures in Cryptol. The signature specifies a function *encrypt* that takes as input an 8-bit or 16-bit integer and output a number of the same size. The quantified type variable *n* in the type

```

1   encrypt: {n} [8] -> String n -> String n
2   // implementation of encryption
3
4   decrypt: {n} [8] -> String n -> String n
5   // implementation of decryption
6
7   encryptCorrect: {n} [8] -> String n -> Bit
8   property encryptCorrect =
9       decrypt key (encrypt key msg) == msg

```

Figure 2.2: Correctness Property in Cryptol

```

1   >> :prove encryptCorrect
2   >> Q.E.D

```

Figure 2.3: Proving Correctness Properties in Cryptol

signature are bounded by the predicates $0 < n$ and $n < 3$. The predicates put a limit on the values of the type variable. Any arithmetic operations can be used in such predicates. Type signatures of these kinds rule out a large number of illegal input statically and provides strong guarantee to the correctness of the program. The AES algorithm [1] for example operates on 128, 192 or 256-bit keys. Such a constraint can precisely specified and checked in Cryptol type system.

Formal Verification and Automated Testing

The Cryptol language provides native formal verification utilities designed for equivalence and safety-checking. Correctness properties can be specified in Cryptol as part of the source code accompanying the algorithm. The Cryptol checker then checks for correctness of properties by means of SAT/SMT solvers. The Z3 prover is used by default.

Figure 2.2 shows a correctness property defined in Cryptol. The property states simply that decryption after encryption with the same key should result in the original message. We can see that a correctness property in Cryptol is but another function that returns a Bit (boolean) type value.

The Cryptol language provides an interactive mode similar to Haskell’s with which developers can test functions interactively. Cryptol can conduct verification of the above property automatically with a simple *:prove* command issued in its interactive prompt, as shown in Figure 2.3.

In cases where the property is invalid, the Cryptol checker provides an input for which the property does not hold true as counterexample. This gives developers a concrete scenario to look into and debug.

```

1      >> :set tests=10000
2      // setting number of test cases generated
3      >> :check encryptCorrect

```

Figure 2.4: Testing Correctness Properties in Cryptol

```

1      >> :sat (\key -> encrypt key msg == cipher)

```

Figure 2.5: Known Plaintext Attack in Cryptol

Because Cryptol properties are just functions, it is possible to write conditions in the property to construct proofs efficiently for more restricted scenarios. For polymorphic functions, we can also restrict its type signatures when proving properties.

Of course it is possible that external theorem prover used by Cryptol could not finish the proof within a reasonable amount of time. Therefore Cryptol also provides another command `:check` that can be used in the same way as `:prove` to conducted automated testing on the property. Figure 2.4 demonstrates how this utility can be used in Cryptol.

Similar to proving correctness, we can check in Cryptol whether a property is satisfiable through the `:sat` command. The command finds a satisfying input for the property using an off-the-shelf SAT solver. Finding satisfying assignments are interesting in cryptography because it can be used to formulate attacks to the cryptographic protocol. Figure 2.5 provides an example of known plain-text attacks specified in Cryptol. Such a property would certainly have a satisfying assignment. The point, however, is that Cryptol should never be able to find that assignment in a feasible amount of time in order for the encryption function to be safe.

2.1.3 How Formal Verification Works in Cryptol

Under the hood, the Cryptol source is translated to a *symbolic bit-vector* language, for which there are existing methods that can then decide if the code segments satisfies a certain property. Translation is done through symbolic evaluation, i.e. by executing the function in question with symbolic variables.

The symbolic bit-vector program can be reduced to a SAT (boolean satisfiability) instance and solved with an off-the-shelf SAT solver such as *lingeling*. For checking equivalence property such as the one in Figure 2.2, we ask the SAT solver if there exists an assignment that would make the property return 0 (false). If there is, then the property does not hold, and part of the assignment will be translated to an input and returned as counterexample for the property. The SAT-based property checking approach has been used to prove equivalence of Cryptol program before and after compiler optimization [17].

Cryptol also supports using SMT (satisfiability modulo theory) solvers in place of SAT solvers to decide the bit-vector programs. The reason why SMT solvers might be better than SAT solvers in this case is that they tend to natively support higher-level structural information and arithmetic operations better than SAT solvers. Many SMT solvers come with dedicated mode for bit-vector programs. In practice, it was found that SMT solvers work better when proving properties that involve algebraic equalities.

2.2 Languages for Cryptographic Applications

The idea of using language features to enhance cryptographic applications have been investigated for over a decade. Some studies, such as [2] builds upon existing languages, and provides extensions, e.g. libraries and frameworks, for efficient implementation of cryptographic protocols. Other like Cryptol [3] create brand-new domain specific programming languages dedicated to cryptographic applications. These works also focus on different aspects of implementation. Some focus on reliability and correctness guarantees, while others emphasize ease of use and performance.

There exist languages that are designed for specific kinds of security protocols. ZKPDL [5], for example, is an interpreted description language for specifying zero-knowledge protocols, motivated by applications such as electronic cash. Although the language is designed specifically for implementing prover and verifier of zero-knowledge, the language itself also have potentials for specifying other types of privacy-preserving systems. The ZKPDL interpreter also performs optimizations for protocols.

Similar to ZKPDL, TASTY [6] is a novel compiler designed specifically for generating efficient two-party computation protocols. TASTY provides a high-level domain specific language in which the user can specify the computation to be performed on encrypted data, and the compiler would translate that directly to a secure protocol. Moreover, TASTY uses the FairPlay [7] system to evaluate the protocol generated.

On the language extension side, NaCl [4] is a C/C++ library for implementing cryptographic protocols that provides security guarantees through features such as no data flow from secrets to load address, and no padding oracles. Charm [2] is an extensible framework in Python designed for rapid prototyping of cryptographic schemes. Charm promotes modularity and re-usability of cryptographic primitives, and successfully increases interoperability of existing numeric libraries such Sage and the Stanford Pairing-Based Crypto (PBC). It also provides benchmarking and profiling utilities for determining the performance of cryptographic algorithms.

The Certified computer-aided cryptography [8] project provides a computer-aided framework for proving concrete security for cryptographic implementations. It extends EasyCrypt, an interactive framework for verifying the security of cryptographic applications, to provide formal verification for cryptographic

Language	Programming Paradigm	Features
Cryptol	Purely Functional	high-level specification, formal verification
CAO [9]	Imperative	high-level specification, performance
cPLC [12]	Imperative	high-level specification, mathematical syntax, numerical libraries

Figure 2.6: Comparing Cryptographic Programming Languages

applications implemented in a C-like language. The framework also supports generation of optimized machine code based on the high-level language while retaining the security properties.

The Cryptol language has a close relative named $\mu\text{Cryptol}$ [13, 14]. The language focuses on providing a verifying compiler that proves the correctness of the code transformation process. Agosta et al. [11] also proposed a domain specific language for cryptography based on Python. The major benefit that this work provides, however, is syntactic.

One of the strongest competitor for Cryptol is CAO [9], a language designed to facilitate high-level, performant implementation of the AES algorithm. The CAO compiler utilizes advanced techniques to improve performance of the implementation, but provides no specific functions for verifying the correctness of the algorithm. There are separate studies on verifying CAO programs such as [10], however the features are not included as a part of the language.

cPLC [12] is a more recent attempt at providing a domain specific languages for cryptography. Instead of borrowing the syntax of existing programming languages, cPLC provides a language that is closed to the mathematical notations used in the cryptography community to describe protocols. Moreover cPLC provides native support for mathematical entities and operations such as groups that are often used in cryptography.

An important feature of Cryptol is that it provides native support for formal verification of cryptographic protocols, a subject that have been studied for decades. We refer to [15] for these works.

Comparing Cryptol with Other Cryptographic Languages

Figure 2.6 compares Cryptol with CAO and cPLC, two of the languages we have covered in Section 2.2. These two languages are chosen because, like Cryptol, they focus on cryptographic applications in general. As shown in the table, Cryptol is the only one that employs a functional programming style, and also the only one that facilitates formal verification. The other two languages, although both high-level languages, put a strong focus on performance of the implementations.

Chapter 3

Implementation and Evaluation

This section presents the implementation part of the project. For the purpose of empirically evaluating the Cryptol language in practice, we created an implementation of the AES algorithm and devised properties to verify the implementation. The AES algorithm is the current standard of symmetric key encryption and is well specified in [1]. A brief introduction to the algorithm and the implementation is provided in Section 3.1. The correctness properties and results of verification is discussed in Section 3.3. In Section 3.4 we summarize the observations of the language from the implementation process.

3.1 The AES Algorithm

We start by providing a brief introduction to the AES algorithm in the section to facilitate our discuss of the implementation.

As a block cipher, the AES algorithm runs on a 4×4 column-major order matrix of bytes. The matrix is formally called a *state* and it has a fixed size of 128 bits. See Figure 3.1 for an example of states.

The other input that the algorithm takes is the encryption key, which can

$$\begin{bmatrix} b_0 & b_4 & b_8 & b_{12} \\ b_1 & b_5 & b_9 & b_{13} \\ b_2 & b_6 & b_{10} & b_{14} \\ b_3 & b_7 & b_{11} & b_{15} \end{bmatrix} \quad (3.1)$$

Figure 3.1: A State in AES

be 128, 192, or 256-bit long. In AES, a sequence of substitution and permutation steps are repeated for a number of rounds, and the number of rounds is decided by the key size. For 128-bit keys, 10 rounds of repetition is required, whereas 12 and 14 rounds are needed for 192-bit and 256-bit keys respectively. The number of rounds are needed to use the encryption key efficiently. More specifically, the algorithm does not simply reuse the encryption key for every round of operations. Instead, the key is expanded into $(\text{number of rounds} + 1)$ round keys, each of which is 128 bits. The expansion is done using Rijndael's key schedule. This way a different round key is used in each round and there is no repetition. Note that because each entry in the state matrix is one byte, most arithmetic operations in Cryptol are defined over a finite field $GF(2^8)$ (GF stands for Galois Field).

In brief there are 5 major functions used in AES:

- *KeyExpansion*: for expanding encryption key to round keys, as we have discussed before.
- *AddRoundKey*: Applying round key to the state using bitwise *xor*.
- *SubBytes*: Substituting each byte in the state according to a lookup table called the S-box.
- *ShiftRows*: Shifting the last three rows of the state cyclically each by different number of bytes.
- *MixColumns*: Transform each column (treated as a polynomial on the field $GF(2^8)$) through matrix multiplication.

Algorithm 1 The AES Algorithm

```

1: roundKeys = expandKey(key)
2:           ▷ roundKeys is an  $n + 1$  array where  $n$  is the number of rounds.
3: state = addRoundKey(state, roundKeys[0])
4: for  $i = 1$  to  $n - 1$  where  $n$  is the number of rounds do
5:   state = subBytes(state)
6:   state = shiftRows(state)
7:   state = mixColumns(state)
8:   state = addRoundKey(state, roundKeys[i])
9: end for
10: state = subBytes(state)
11: state = shiftRows(state)
12: state = addRoundKey(state, roundKeys[n])
13:           ▷ The last round does not involve the MixColumns operation.
14: return state

```

We refer to [1] for more detailed description of these operations. Algorithm 1 shows the pseudo-code for the algorithm using the operations introduced. The decryption function is simply the reverse of the encryption function, and is made up of operations and rounds that reverse the operations and rounds of the encryption function.

```
1 type State = [4][4][8]
```

Figure 3.2: Defining the State type in Cryptol

```
1 xs = [1 .. 10] // a list of numbers
2 ys = [0] # [ y + x | x <- xs
3             | y <- ys ]
4 // ys = [0, 1, 3, ..., 55]
```

Figure 3.3: A Loop Written in Fold in Cryptol

3.2 Implementation Details

We present below a few language features that are prominently used in our implementation.

Type Synonyms

Remember that size of input is specified in the type signature. In Cryptol, we can define type synonyms to improve re-usability and readability, just like in Haskell. The major data structures in AES are defined as type synonyms in Cryptol in our implementation. Remember that a State in Cryptol is a 4×4 matrix of bytes. An example of the State type is shown in Figure 3.2.

Fold

As a functional programming language, Cryptol provides no supports for writing for-loop or while-loop. The only natural way of writing a loop in Cryptol, besides recursive functions is *fold*. In functional programming, fold is a way to recursively analyze a data structure such as a list, combine the results of each iteration and accumulatively build up a return value. See Figure 3.3 for an example of loops written with *fold* in Cryptol. This is a function that computes the sum of the list *xs*. Note that the variable *ys* is used in its own definition. This is similar to a *foldr* function in Haskell [18]. The result, however, in this case is a list that includes the value of each intermediate step.

Folds are the recommended way of writing loops in Cryptol, and therefore are frequently used in our implementation.

3.3 Implementation and Verification

Using a pure functional language such as Cryptol to implement the AES algorithm, fortunately does not result in any complications more than necessary.

```

1  type State = [4][4][8]
2  type RoundKey = State
3  type KeySize = 128      // 192, 256
4
5  // encryption functions
6  subBytes : State -> State
7  shiftRows: State -> State
8  mixColumns: State -> State
9  addRoundKey: RoundKey -> State -> State
10 encrypt: [128] -> [KeySize] -> [128]
11
12 // decryption functions
13 reverseSubBytes: State -> State
14 reverseShiftRows: State -> State
15 reverseMixColumns: State -> State
16 decrypt: [128] -> [KeySize] -> [128]

```

Figure 3.4: Function Signatures of Major AES Operations

Each major operation can be implemented as a pure function, i.e. one that is free of side effects, and of course the eventual encryption and decryption functions are also side-effect free.

In Figure 3.4 we list type signatures of the major functions in AES. This provides a high-level overview of our implementation. Note how well this corresponds to the description of AES in Section 3.1. All the major operations transform the *State* type. The encryption and decryption functions work on 128-bit plain text, and takes as input a key that is either 128, 192, or 256-bit long. Of course these are not the only functions and types in the implementation. There are many more helper functions such as those for computing multiplicative inverse on a finite field and for matrix multiplication. We also implement multiple versions of the same function where possible, so that these different versions can be used to verify each other. This is conducted under the assumption that with the correct specification, the same mistake is unlikely to be made in two different versions.

The next step is naturally verifying our implementation. This is however not as straight-forward as the example shown in Figure 2.2, because high-level properties defined directly over the encryption and decryption functions generally take too long to prove. This is likely because the AES algorithm has an intentionally large state space, and the purpose of the algorithm is to obfuscate and make it computationally impossible to analyze the relationship between the input and the output. Therefore instead of verifying the encryption and decryption functions as a whole, we adopt a different strategy: verify each component of the algorithm separately. As the composition of components is pretty straight-forward for AES, this approach would provide strong guarantee that the implementation is correct.

A set of correctness properties are defined in order to verify the implemen-

tation. These properties for functions are designed using the three strategies:

- Verifying important properties intrinsic to the functions;
- Verifying equivalence of different versions of the same function;
- Verifying that the reverse functions successfully undo the encrypt functions

Many of the basic functions have important properties that can be used to verify them, and many of these properties can be proved efficiently. For example, the product of a number and its multiplicative inverse on a finite field equals to 1. This property is the defining characteristic of multiplicative inverse and can be used to verify the function. Similarly we verify commutativity and associativity for finite field multiplication.

Moreover, the AES specification sometimes provide optimization such as look-up table that replaces computation steps. We implement some of these optimizations and ask Cryptol to check equivalence of the optimized and original functions. This is the approach taken for functions such as *subBytes*.

Another way to ensure correctness is make sure that reverse operations used in the decryption function can actually cancel out their corresponding operations in the encryption function. This is approach is used to verify *shiftRows* for example.

In complement with formal verification, we use the automated testing utility provided in Cryptol to test the properties that are defined, especially when the properties could not be proved in a feasible amount of time.

Figure 3.5 summarizes the result of the formal verification process. The result is largely positive: most of the properties can be efficiently proved, while the rest passed the automated tests at least. This gives us a strong confidence that the implementation is correct.

The program is implemented and verified using Cryptol 2.2.6 on Ubuntu 16.04. For instructions on installing Cryptol and running the source code, please refer to the *README.md* included in the project.

3.4 Review of the Cryptol Language

In this section we summarize our observations of the Cryptol language from the both the literature survey and the implementation project.

First of all, Cryptol is a very unique solution to programming language for cryptography. As we have seen in Section 2.2, it is not the only language that have been designed specifically for cryptography. However Cryptol is the only pure functional language that has been proposed. Moreover, its native support

Property	Description	Result
<i>polySelfAdd</i>	the sum of two same polynomials on $GF(2^*)$ is 0	proved
<i>mulIden</i>	any number multiplied with the identity element over the field equals the number itself	proved
<i>mulCommutative</i>	commutative property of field multiplication	proved
<i>mulAssociate</i>	associative property of field multiplication	proved
<i>mulInverseCorrect</i>	multiplicative inverse's definition	proved
<i>subByteCorrect</i>	two versions of subBytes are equivalent	proved
<i>shiftRowsCorrect</i>	<i>shiftRows</i> applied 4 times results in the original state	proved
<i>rConCorrect</i>	two versions of round constants are equivalent	tested
<i>formByteCorrect</i>	verify <i>formByte</i> against its reverse function	proved
<i>toFromStateCorrect</i>	toState is the reverse of fromState	proved
<i>reverseShiftRows</i>	verify <i>shiftRows</i> against its reverse function	proved
<i>mixColumnsCorrect</i>	verify <i>mixColumns</i> against its reverse function	tested
<i>aesCorrect</i>	decrypt (encrypt (m, k), k) == m	tested

Figure 3.5: Correctness Properties and Results of Verification

for formal verification is also unique. These features all make it stand out as a programming language for cryptography.

Specifying correctness properties in Cryptol is easy as the properties are eventually just functions. Verification is reasonably fast for most basic functions. The precise type system also provides very good compiler-time guarantees: if the program compiles, it can probably run without errors.

The language also naturally promotes modularity and readability. The implementation of the AES algorithm in Cryptol, even after including multiple versions of some functions, are still shorter than the equivalent implementation in C or Java. The size of the source code could be reduced even more should it be desired. This however is not the purpose of the project, and therefore not attempted. The functional programming style works well for encryption and decryption algorithms as they are often by design pure functions.

However as a relative young language, there are still a few caveats with the language. We discuss these issue below.

Proving Polymorphic Properties

Cryptol does not support verifying properties with polymorphic types, because the properties might hold for some type instances but not others. This however doesn't mean polymorphic types are useless in properties. It is just that when asking Cryptol to prove these properties, the developers must provide extra, monomorphic type signature for the prover to work.

Branching

The if statement is often the only solution to writing conditions in Cryptol. The advantage of this is that the algorithms specified in an imperative style can often be translated with ease. However, whether this is a good language feature is a matter of debate. The language does provide pattern matching, however it is not as powerful as that in Haskell, and is used to only access components of data structures. A more powerful pattern matching feature like that of Haskell's is desirable.

Lack of Support for Floating Point Number

Cryptol has no native support for floating-point number. This is in fact not a big problem for many cryptographic algorithms, especially symmetric key cryptographic algorithms, as they operate primarily on integers defined over finite fields. However floating-point number can be useful when experimenting on advanced public key cryptographic algorithms, e.g. those using elliptic curves.

Limited Standard Library

As a language designed for cryptography, Cryptol's standard library lacks

functions that are common and useful for many cryptographic algorithms. During the implementation project, it was often necessary to implement basic functions that are often seen in cryptography. Arithmetic operations (addition, multiplication, exponentiation, etc.) on finite fields is one example. The cPLC [12] language, for example, comes with support for a number of mathematical functions that are useful for developing cryptographic algorithms. With rapid prototyping being one of the design objectives of the Cryptol language, it would be a good idea to include basic number theoretical utilities in the standard library.

Chapter 4

Conclusion and Future Works

In the project proposal we set out a concrete time frame for the project. The project adhered to the schedule closely, and everything that was planned in the proposal, including both the literature survey and the implementation was completed on time. A large number of properties that were devised were successfully proved on the implementation. The rest also passed the automated tests at least.

More importantly, the project provides valuable insight to the language itself. From the survey and implementation we came to the conclusion that Cryptol is a plausible language for cryptography. The language allows for very high-level specification of algorithms. The native support for formal verification is very useful for development of cryptographic algorithms. The precise type system is also helpful. However there are still issues, such as the lack of a comprehensive standard library, to be resolved for the language to gain traction.

As a relatively young language, Cryptol has a lot of potential to be developed. One of the possibility discussed in [3] is that of compiling the Cryptol source code into target languages and platforms such as C, Java, or even assembly. This however is not supported in the current version of Cryptol. The Software Analysis Workbench (SAW), a tool developed by the same organization Galois Inc., also provides utility for proving equivalence of Cryptol functions and Java or C functions. Similar to Cryptol's property prover. SAW utilizes symbolic execution to translate programs into formal models. This means that the Cryptol implementation of an algorithm can be used to verify implementations in other languages. It is however not as easy as it sounds, as the equivalence checking is only possible when the function design (type signature etc.) is similar in these language. That is not necessarily the case as Cryptol is a functional language, whereas C and Java are imperative, and object-oriented. Therefore whether the SAW toolset can be used to effectively verify C and Java source code is a matter to be investigated.

It should also be noted that even if a cryptographic algorithm is proved to be correct based on a certain specification, it still does not mean that the algorithm is secure. At the moment, there is no way to prove security in Cryptol, which is not an actual problem of the language. Automated proof for security is a hard problem with no general solution, especially when there are many different notions of security such as IND-CPA (indistinguishability under chosen plaintext attack) and IND-CCA (indistinguishability under chosen ciphertext attack). This is simply something for developers to keep in mind, and can perhaps be an interesting topic of research.

Bibliography

- [1] N.-F. Standard, “Announcing the advanced encryption standard (aes),” *Federal Information Processing Standards Publication*, vol. 197, pp. 1–51, 2001.
- [2] J. A. Akinyele, C. Garman, I. Miers, M. W. Pagano, M. Rushanan, M. Green, and A. D. Rubin, “Charm: a framework for rapidly prototyping cryptosystems,” *Journal of Cryptographic Engineering*, vol. 3, no. 2, pp. 111–128, 2013.
- [3] J. R. Lewis and B. Martin, “Cryptol: High assurance, retargetable crypto development and validation,” in *Military Communications Conference, 2003. MILCOM’03. 2003 IEEE*, vol. 2, pp. 820–825, IEEE, 2003.
- [4] D. J. Bernstein, T. Lange, and P. Schwabe, “The security impact of a new cryptographic library,” in *International Conference on Cryptology and Information Security in Latin America*, pp. 159–176, Springer, 2012.
- [5] S. Meiklejohn, C. C. Erway, A. Küpçü, T. Hinkle, and A. Lysyanskaya, “Zkpd: A language-based system for efficient zero-knowledge proofs and electronic cash,” in *USENIX Security Symposium*, vol. 10, pp. 193–206, 2010.
- [6] W. Henecka, A.-R. Sadeghi, T. Schneider, I. Wehrenberg, *et al.*, “Tasty: tool for automating secure two-party computations,” in *Proceedings of the 17th ACM conference on Computer and communications security*, pp. 451–462, ACM, 2010.
- [7] D. Malkhi, N. Nisan, B. Pinkas, Y. Sella, *et al.*, “Fairplay-secure two-party computation system,” in *USENIX Security Symposium*, vol. 4, San Diego, CA, USA, 2004.
- [8] J. B. Almeida, M. Barbosa, G. Barthe, and F. Dupressoir, “Certified computer-aided cryptography: efficient provably secure machine code from high-level implementations,” in *Proceedings of the 2013 ACM SIGSAC conference on Computer & communications security*, pp. 1217–1230, ACM, 2013.

- [9] A. Moss and D. Page, “Bridging the gap between symbolic and efficient aes implementations,” in *Proceedings of the 2010 ACM SIGPLAN workshop on Partial evaluation and program manipulation*, pp. 101–110, ACM, 2010.
- [10] M. Barbosa, J. Pinto, J.-C. Filliâtre, and B. Vieira, “A deductive verification platform for cryptographic software,” *Electronic Communications of the EASST*, vol. 33, 2010.
- [11] G. Agosta and G. Pelosi, “A domain specific language for cryptography,” in *FDL*, pp. 159–164, Citeseer, 2007.
- [12] E. Bangerter, S. Krenn, M. Seifriz, and U. Ultes-Nitsche, “cplca cryptographic programming language and compiler,” in *2011 Information Security for South Africa*, pp. 1–8, IEEE, 2011.
- [13] M. Shields, “A language for symmetric-key cryptographic algorithms and its efficient implementation,” *Available from the authors website*, 2006.
- [14] L. Pike, M. Shields, and J. Matthews, “A verifying core for a cryptographic language compiler,” in *Proceedings of the sixth international workshop on the ACL2 theorem prover and its applications*, pp. 1–10, ACM, 2006.
- [15] C. A. Meadows, “Formal verification of cryptographic protocols: A survey,” in *International Conference on the Theory and Application of Cryptology*, pp. 133–150, Springer, 1994.
- [16] R. Hindley, “The principal type-scheme of an object in combinatory logic,” *Transactions of the american mathematical society*, vol. 146, pp. 29–60, 1969.
- [17] L. Erkök and J. Matthews, “Pragmatic equivalence and safety checking in cryptol,” in *Proceedings of the 3rd workshop on Programming Languages meets Program Verification*, pp. 73–82, ACM, 2009.
- [18] M. Lipovaca, *Learn You a Haskell for Great Good!: A Beginner’s Guide*. no starch press, 2011.