The following full text is a preprint version which may differ from the publisher's version.

For additional information about this publication click this link.
http://hdl.handle.net/2066/132669

Please be advised that this information was generated on 2017-08-31 and may be subject to change.
Abstract. This paper presents results on formal verification of high-speed cryptographic software. We consider speed-record-setting hand-optimized assembly software for Curve25519 elliptic-curve key exchange in [11]. Two versions for different microarchitectures are available. We successfully verify the core part of computation, and reproduce a bug in a previously published edition. An SMT solver for the bit-vector theory is used to establish almost all properties. Remaining properties are verified in a proof assistant. We also exploit the compositionality of Hoare logic to address the scalability issue. Essential differences between both versions of the software are discussed from a formal-verification perspective.

1 Introduction

Cryptography is the backbone of modern information security. Implementations of cryptographic primitives now form key software libraries which are run all the time, everywhere, by all kind of computers big and small. It makes sense to optimize crypto software at the assembly level because repetitive portions of programs are tiny (e.g., the inner loop of AES or Advanced Encryption Standard which encodes terabytes every day has but a few lines). Inefficiency may also translate directly into insecurity, by forcing a scale-down of the primitive due to usability concerns [18, Sec. 9, p. 5]. Finally, information leaks such as dependency of execution time on secret data violates the model of security, and such leaks are easier to avoid with hand-crafted assembly instructions. Keys in earlier Linux kernel disk encryption can leak in 65ms [31, 33] due to such timing attacks.

It is important that critical software components in any domain be correct, and the cost of failure for crypto libraries is uniquely magnified further by users being adversarial – i.e., whereas bugs are stumbled upon accidentally in normal use for most software, attackers

⋆ This work was supported by the National Science Foundation under grant 1018836 and by the Netherlands Organisation for Scientific Research (NWO) through Veni 2013 project 13114. Permanent ID of this document: 55ab668ce87d857c02a5b2d56d7da38. Date: 2014.04.28.; it was supported by the Academia Sinica Institute of Information Science under BY's Specialty Project and Career Advancement Award.
routinely seek them out and exploit them to filch secrets [16]. Hand-crafted highly optimized assembly makes thorough code auditing extremely tedious and time consuming. It would be ideal if one could take such a cryptographic library and formally verify it to be correct (and even free of instructions which might time differently depending on secret data).

In this paper, we report results on verifying the correctness of such an implementation for the Curve25519 elliptic-curve Diffie-Hellman key-exchange protocol [10], which had initially set speed records for key exchange at the 128-bit security level for 32-bit Intel processors. Cryptography on this curve has since become something of a reference point for the “high-speed-crypto” community, having seen highly optimized implementations for diverse architectures, including the Cell Broadband Engine and the ARM Cortex-A8 [19,14].

Curve25519 has also seen wide adoption from the applied-security community, including Tor [32] (switching from RSA-1024 for speed and security [27]!), Apple’s iOS operating system [5], the Networking and Cryptography library (NaCl) [13], and the latest version of OpenSSH [1]. In addition, it is being considered by an IETF draft [25] for inclusion into TLS (https).

New record speeds for standard 64-bit Intel and AMD processors were set by Gaudry and Thomé [22] and later by Bernstein, Duif, Lange, Schwabe, and Yang [11,12], currently still the fastest Curve25519 implementation on 64-bit Intel and AMD processors. This speed record holder (without conditional branches or secret-index table look-ups) is the target for verification in this paper.

To achieve our goals, we propose a methodology that integrates compositional reasoning, SMT solvers, and proof assistants. Elliptic-curve cryptography performs arithmetic operations in large finite fields. Any verification has to analyze tens of non-linear arithmetic operations on values with hundreds of bits. Despite significant developments in the past decade, such tasks are still infeasible for SMT solvers to verify automatically. Proof assistants, on the other hand, require significant human guidance. Analyzing thousands of low-level assembly instructions is perhaps too inhumane for average enthusiasts.

We attempt to get the best out of these techniques in our integrated methodology. Applying the compositional proof rule in Hoare logic, we divide low-level implementations of cryptographic software into parts. The SMT solver Boolector is used to establish low-level properties of each part automatically. For instance, it is very feasible to verify automatically that instructions are free of overflow, although it can be extremely difficult to prove that the same instructions perform modular multiplication over a large finite field. After low-level properties are established, we use the proof assistant Coq to verify high-level arithmetic properties about cryptographic software. Thanks to SMT solvers, it is not needed to show manually that low-level properties such as free-of-overflow do not occur. Proof assistants can focus on algebraic properties such as modular congruence. Human efforts are thus significantly reduced.

In short, we propose a hybrid methodology that is more scalable than pure SMT solving and theorem proving. With our methodology, we have verified the Montgomery ladder step of a speed-record-holding implementation of the widely used Curve25519 key exchange protocol. The Montgomery ladder step consists of 1277 and 1383 low-level instructions in the radix-2^{64} and radix-2^{51} implementations respectively. To the best of our knowledge, we believe this work is the first on formal verification of the core computation of manually optimized low-level implementations for a real-world cryptographic protocol.
Related work. In [3], a SmartMIPS (a superclass of MIPS32) implementation for a pseudorandom-number generator is formally proved to be cryptographically secure with the proof assistant Coq. The authors adopt the formalization of MIPS32 instructions in [2] and give a formal reduction proof for their own implementation of the pseudorandom number generator. We combine automatic SMT solvers and proof assistants to verify the core computation of a record-holding implementation of a real-world security protocol. We do not address the security issues in this work, but the scale and impact can be far more significant.

The project CryptVer aims to verify implementations of cryptographic algorithms written in an efficient high-level language [23]. Their approach is to specify cryptographic algorithms and implement them by formal deductive compilation. In contrast, we formally verify manually optimized low-level implementations for cryptographic software. Equivalence checking of low-level code for digital signal processing is discussed in [20]. The authors compare implementations with golden models. We verify the correctness of low-level code directly.

Another approach to formally verified cryptographic software are special-domain compilers. A recent example of this is [4], where Almeida et al. introduce security-aware compilation of a subset of the C programming language.

As stated before, cryptographic software must be more than correct, it must avoid information leaks against its security model, i.e., be “side-channel resistant”. As a consequence, countermeasures against side-channel attacks have also been formalized. For example, Bayrak et al. [7] use SAT solving for the automated verification of power-analysis countermeasures. Molnar et al. [29] describe a tool for static analysis for control-flow vulnerabilities and their automatic removal.

Organization of this paper. Section 2 gives the necessary background on Curve25519 elliptic-curve Diffie-Hellman key exchange. Section 3 reviews the two different approaches for assembly implementations of arithmetic in the field $\mathbb{F}_{2^{255}-19}$ used in [11]. Section 4 gives an overview of the tools we use for verification. Section 5 details our methodology. Section 6 presents and discusses our results. We conclude the paper and point to future work in Section 7.

2 Curve25519

Cryptography based on the arithmetic on elliptic curves was proposed independently by Miller and Koblitz [26,28]. We only give a very brief introduction to elliptic-curve cryptography here; please refer to (for example) [6,24] for more information.

Let $\mathbb{F}_q$ be the finite field with $q$ elements. For $a_1, a_2, a_3, a_4, a_6 \in \mathbb{F}_q$, an equation of the form $E : y^2 + a_1 xy + a_3 y = x^3 + a_2 x^2 + a_4 x + a_6$ defines an elliptic curve $E$ over $\mathbb{F}_q$ (with certain conditions, cf. [24, Chapter 3]). The set of points $(x, y) \in \mathbb{F}_q \times \mathbb{F}_q$ together with a “point at infinity” form a group of size $\ell \approx q$, usually written additively. The group law is efficiently computable through a few operations in the field $\mathbb{F}_q$, so given a point $P$ and a scalar $k \in \mathbb{Z}$ it is easy to do a scalar multiplication $k \cdot P$, which requires a number of addition operations that is linear in the length of $k$ (i.e., logarithmic in $k$).

In contrast, for a sufficiently large finite field $\mathbb{F}_q$, a suitably chosen curve, and random points $P$ and $Q$, computing the discrete logarithm $\log_P Q$, i.e., to find $k \in \mathbb{Z}$ such that $Q = k \cdot P$, is hard. More specifically, for elliptic curves used in cryptography, the best known algorithms takes time $\Theta(\sqrt{\ell})$. Elliptic-curve cryptography is based on this difference in the complexity for computing scalar multiplication and computing discrete logarithms. A user
who knows a secret $k$ and a system parameter $P$ computes and publishes $Q = k \cdot P$. An attacker who wants to break security of the scheme needs to obtain $k$, i.e., compute $\log_P Q$.

Curve25519 is an elliptic-curve Diffie-Hellman key exchange protocol proposed by Bernstein in 2006 [10]. It is based on arithmetic on the elliptic curve $E : y^2 = x^3 + 486662x^2 + x$ defined over the field $\mathbb{F}_{2^{255} - 19}$.

2.1 The Montgomery ladder

Scalar multiplication in Curve25519 uses a so-called differential-addition chain proposed by Montgomery in [30] that uses only the $x$-coordinate of points. It is highly regular, performs one ladder step per scalar bit, and can be run in constant time; the whole loop is often called Montgomery ladder. An overview of the structure of the Montgomery ladder and the operations involved in one ladder-step are given respectively in Algs. 1 and 2. The inputs and outputs $x_P, X_1, X_2, Z_2, X_3, Z_3$, and temporary values $T_i$ are elements in $\mathbb{F}_{2^{255} - 19}$. The performance of the computation is largely determined by the performance of arithmetic operations in this field.

Algorithm 1 Curve25519 Montgomery Ladder

Input: A 255-bit scalar $k$ and the $x$-coordinate $x_P$ of a point $P$ on $E$.
Output: $(X_{kP}, Z_{kP})$ fulfilling $x_{kP} = X_{kP}/Z_{kP}$

$t = \lceil \log_2 k + 1 \rceil$

$X_1 = x_P; X_2 = 1; Z_2 = 0; X_3 = x_P; Z_3 = 1$

for $i \leftarrow t - 1$ downto 0 do

if bit $i$ of $k$ is 1 then

$(X_3, Z_3, X_2, Z_2) \leftarrow \text{ladderstep}(X_1, X_3, Z_3, X_2, Z_2)$

else

$(X_2, Z_2, X_3, Z_3) \leftarrow \text{ladderstep}(X_1, X_2, Z_2, X_3, Z_3)$

end if

end for

return $(X_2, Z_2)$

The biggest difference between the two Curve25519 implementations of Bernstein et al. presented in [11,12] is the representation of elements of $\mathbb{F}_{2^{255} - 19}$. Both implementations have the core parts, the Montgomery ladder step, in fully inlined, hand-optimized assembly. These core portions are what we target for verification in this paper.

3 $\mathbb{F}_{2^{255} - 19}$ arithmetic in AMD64 assembly

Arithmetic in $\mathbb{F}_{2^{255} - 19}$ means addition, subtraction, multiplication and squaring of 255-bit integers modulo the prime $p = 2^{255} - 19$. No mainstream computer architecture offers arithmetic instructions for 255-bit integers directly, so operations on such large integers must be constructed from instructions that work on smaller data types. The AMD64 architecture has instructions to add and subtract (with and without carry/borrow) 64-bit integers, and the MUL instruction returns the 128-bit product of two 64-bit integers, always in general-purpose registers rdx (higher half) and rax (lower half).

Section 3 of [11] describes two different approaches to implement $\mathbb{F}_p$ arithmetic in AMD64 assembly. Both approaches use the 64-bit-integer machine instructions. They are different
Algorithm 2 One “step” of the Curve25519 Montgomery Ladder

function ladderstep(\(X_1, X_2, Z_2, X_3, Z_3\))
\[\begin{align*}
T_1 &\leftarrow X_2 + Z_2 \\
T_2 &\leftarrow X_2 - Z_2 \\
T_7 &\leftarrow T_2^2 \\
T_6 &\leftarrow T_7^2 \\
T_5 &\leftarrow T_6 - T_7 \\
T_3 &\leftarrow X_3 + Z_3 \\
T_4 &\leftarrow X_3 - Z_3 \\
T_9 &\leftarrow T_3 \cdot T_2 \\
T_8 &\leftarrow T_4 \cdot T_1 \\
X_3 &\leftarrow (T_8 + T_9) \\
Z_3 &\leftarrow (T_8 - T_9) \\
X_3 &\leftarrow X_3^2 \\
Z_3 &\leftarrow Z_3^2 \\
Z_3 &\leftarrow Z_3 \cdot X_1 \\
X_2 &\leftarrow T_6 \cdot T_7 \\
Z_2 &\leftarrow 121666 \cdot T_5 \\
Z_2 &\leftarrow Z_2 + T_7 \\
Z_2 &\leftarrow Z_2 \cdot T_5 \\
\text{return } (X_2, Z_2, X_3, Z_3)
\end{align*}\]
end function

in the representation of elements of \(\mathbb{F}_p\), i.e., they decompose the 255-bit field elements into smaller pieces which fit into 64-bit registers in different ways. We now review these approaches and highlight the differences that are most relevant to verification.

3.1 Field arithmetic in radix-\(2^{64}\) representation

The obvious representation of an element \(X \in \mathbb{F}_p\) (or any 256-bit number) with 64 bit integers is \(\textit{radix} \ 2^{64}\). A 256-bit integer \(X\) is represented by 4 64-bit unsigned integers \((x_0, x_1, x_2, x_3)\), where the \(\text{limbs}\) \(x_i \in \{0, \ldots, 2^{64} - 1\}\) and

\[X = \sum_{i=0}^{3} x_i 2^{64i} = x_0 + 2^{64} x_1 + 2^{128} x_2 + 2^{192} x_3.\]

We will focus our description on the most complex \(\mathbb{F}_p\) operation in the Montgomery ladder step, which is multiplication. Squaring is like multiplying, except that some partial results are known to be the same and computed only once. Addition and subtraction are straightforward and multiplication by a small constant simply foregoes computation of results known to be zero. Multiplication in \(\mathbb{F}_p\) consists of two steps: multiplication of two 256-bit integers to produce a 512-bit intermediate result \(S\), and reduction modulo \(2p\) to obtain a 256-bit result \(R\). Note that the software does not perform a full reduction modulo \(p\), but only requires that the result fits into 256 bits.

**Multiplication of 256-bit integers.** The approach for multiplication in \(\text{radix-} 2^{64}\) chosen by [11] is a simple schoolbook approach. Multiplication of two 256-bit integers \(X\) and \(Y\) can be seen as a 4-step computation which in each step involves one limb of \(Y\) and all limbs of \(X\) as follows:

\[A_0 = X y_0, \ A_1 = 2^{64} X y_1 + A_0, \ A_2 = 2^{128} X y_2 + A_1, \ S = A_3 = 2^{192} X y_2 + A_2.\]  \(1\)
Each step essentially computes and accumulates the 5-limb partial product \(Xy_i\) with 4 64 \times 64\)-bit multiplications and several additions as \((x_0y_i + 2^{64}x_1y_i + 2^{128}x_2y_i + 2^{192}x_3y_i, t_0 + t_1)\). Note that “multiplications by \(2^{64}\)” are free and only determine where to add when summing 128-bit products. For example, the result of \(x_0y_i\) is in two 64-bit registers \(t_0\) and \(t_1\) with \(x_0y_i = 2^{64}t_0 + t_1\), therefore \(t_1\) needs to be added to the lower result register of \(x_1y_i\) which in turn produces a carry bit which must go into the register holding the higher half of \(x_1y_i\).

Instructions adding \(A_{i-1}\) into \(A_i\) also produce carry bits that need to be propagated through the higher limbs.

Handling the carry bits, which occur inside the radix-\(2^{64}\) multiplication, incurs significant performance penalties on some microarchitectures as detailed in [11, Section 3]. In Sec. 6 we will explain why integrated multiplication and handling of carry bits also constitutes a major obstacle for formal verification.

**Modular reduction.** The multiplication of the two 256-bit integers \(X\) and \(Y\) produced a 512-bit result in \(S = (s_0, \ldots, s_7)\). Now \(S\) must be reduced modulo \(2p = 2^{256} - 38\). We will use repeatedly that \(2^{536} \equiv 38 \pmod p\). The initial step of reduction is to compute

\[
S' = (s_0 + 2^{64}s_1 + 2^{128}s_2 + 2^{192}s_3) + 38 \cdot (s_4 + 2^{64}s_5 + 2^{128}s_6 + 2^{192}s_7)
\]

with a 5-limb result \(S' = (s'_0 + 2^{64}s'_1 + 2^{128}s'_2 + 2^{192}s'_3 + 2^{256}s'_4)\). Note that the highest limb \(s'_4\) of \(S'\) has at most 6 bits. A subsequent step computes

\[
S'' = (s'_0 + 2^{64}s'_1 + 2^{128}s'_2 + 2^{192}s'_3) + 38s'_4
\]

The value \(S'' = (s''_0 + 2^{64}s''_1 + 2^{128}s''_2 + 2^{192}s''_3 + 2^{256}s''_4)\) may still have 257 bits, i.e., \(s''_4\) is either zero or one. The final 4-limb result \(R\) is obtained as

\[
R = (s''_0 + 2^{64}s''_1 + 2^{128}s''_2 + 2^{192}s''_3) + 38s''_4.
\]

### 3.2 Field arithmetic in radix-\(2^{51}\) representation

Due to the performance penalties in handling carries, [11] proposes to represent elements of \(\mathbb{F}_p\) in radix \(2^{51}\), i.e., \(X \in \mathbb{F}_p\) is represented by 5 limbs \((x_0, \ldots, x_4)\) as

\[
X = \sum_{i=0}^{4} x_i 2^{51i} = x_0 + 2^{51}x_1 + 2^{102}x_2 + 2^{153}x_3 + 2^{204}x_4.
\]

Every element of \(\mathbb{F}_p\) can be represented with all \(x_i \in [0, 2^{51} - 1]\); however, inputs, outputs, and intermediate results inside the ladder step have relaxed limb-size restrictions. For example, inputs and outputs of the ladder step have limbs in \([0, 2^{51} + 2^{15}]\). Additions are done limbwise, e.g., after the first operation \(T_1 \leftarrow X_2 + Z_2\), the limbs of \(T_1\) have at most 53 bits. Substractions are done by first adding a multiple of \(p\) guaranteed to exceed the subtrahend limbwise. For example, the subtraction \(T_2 \leftarrow X_2 - Z_2\) is done by first adding \(0xFFFFFFFFFFFFFD\) to the lowest limb of \(X_2\) and \(0xFFFFFFFFFFFFFE\) to the four higher limbs of \(X_2\), and then subtracting corresponding limbs of \(Z_2\). The value added is \(2p\), which does not change the result (as element of \(\mathbb{F}_p\)), yet ensures that all limbs of the result \(T_2\) are positive and have at most 53 bits.

The most complex operation—multiplication—is split in two parts, but these now differ from those of Sec. 3.1. The first step performs multiplication and modular reduction; the second step performs the delayed carries.
Multiply-and-Reduce in radix-$2^{51}$. To multiply $X = x_0 + 2^{51}x_1 + 2^{102}x_2 + 2^{153}x_3 + 2^{204}x_4$ and $Y = y_0 + 2^{51}y_1 + 2^{102}y_2 + 2^{153}y_3 + 2^{204}y_4$, start by precomputing $19y_1, 19y_2, 19y_3$ and $19y_4$, then compute 5 intermediate values $s_0, \ldots, s_4$, each in two 64-bit registers, as

$$
\begin{align*}
  s_0 & := x_0y_0 + x_1(19y_1) + x_2(19y_3) + x_3(19y_2) + x_4(19y_1), \\
  s_1 & := x_0y_1 + x_1y_0 + x_2(19y_4) + x_3(19y_3) + x_4(19y_2), \\
  s_2 & := x_0y_2 + x_1y_1 + x_2y_0 + x_3(19y_4) + x_4(19y_3), \\
  s_3 & := x_0y_3 + x_1y_2 + x_2y_1 + x_3y_0 + x_4(19y_4), \\
  s_4 & := x_0y_4 + x_1y_3 + x_2y_2 + x_3y_1 + x_4y_0.
\end{align*}
$$

(2)

Note that all partial results in this computation are significantly smaller than 128 bits. For example, when $0 \leq x_i, y_i < 2^{54}$ (input limbs are at most 54-bits), $0 \leq s_0, s_1, s_2, s_3, 19s_4 < 95 \cdot 2^{108} < 2^{115}$. Thus, adding of multiplication results can be achieved by two 64-bit addition instructions (one with carry); carry bits from these additions are collected by the “free” bits of the higher register of $s_i$.

Now $X \cdot Y = S = s_0 + 2^{51}s_1 + 2^{102}s_2 + 2^{153}s_3 + 2^{204}s_4$, but the limbs $s_i$ are still two-register values, much too large to be used in subsequent operations.

Delayed carry. For a 2-register value $s_i$, let $s_i^{(l)}$ denote the lower register and $s_i^{(h)}$ the higher register, i.e., $s_i = s_i^{(l)} + 2^{51}s_i^{(h)}$. Carrying from $s_i$ to $s_{i+1}$ is done as follows: Shift $s_i^{(l)}$ to the left by 13 and shift the 13 high bits of $s_i^{(l)}$ into the 13 low bits of the result. This operation is just one `SHLD` instruction. Now set the high 13 bits of $s_i^{(l)}$ to zero (logical `AND` with $2^{51} - 1$).

Now do the same shift-by-13 operation on $s_{i+1}^{(h)}$ and $s_i^{(l)}$, set the high 13 bits of $s_{i+1}^{(l)}$ to zero, add $s_i^{(h)}$ to $s_{i+1}^{(l)}$ and discard $s_i^{(h)}$. This carry chain is performed from $s_0$ through $s_4$; then $s_4^{(h)}$ is multiplied by 19 (using a `single-word MUL`) and added to $s_0^{(l)}$.

Note: We need $s_i^{(h)} < 2^{51}$ to begin this operation so as not to lose bits from $s_i^{(h)}$ in the shift-by-13. Due to the multiply by 19 at the end, $s_4^{(h)}$ must be even smaller, but the expression for $s_4$ does not already have a multiply by 19 in Eq. 2, so we can guarantee no overflows if limbs of $X$ and $Y$ are at most 54 bits.

This first step of carrying yields $XY = s_0^{(l)} + 2^{51}s_1^{(l)} + 2^{102}s_2^{(l)} + 2^{153}s_3^{(l)} + 2^{204}s_4^{(l)}$, but the values in $s_i^{(l)}$ may still be too big as subsequent operands.

A second carry copies $s_0^{(l)}$ to a register $t$, shifts $t$ to the right by 51, adds $t$ to $s_1^{(l)}$ and discards the upper 13 bits of $s_0^{(l)}$. Carrying continues this way from $s_1^{(l)}$ to $s_2^{(l)}$, from $s_2^{(l)}$ to $s_3^{(l)}$, and from from $s_3^{(l)}$ to $s_4^{(l)}$. Finally $s_4^{(l)}$ is reduced in the same way; except that 19$t$ is added to $s_0^{(l)}$. This produces the final result

$$
R = (s_0^{(l)} + 2^{51}s_1^{(l)} + 2^{102}s_2^{(l)} + 2^{153}s_3^{(l)} + 2^{204}s_4^{(l)}).
$$

4 Tools Used to Verify Curve25519

4.1 Portable assembly: qasm

The software we are verifying has not been written directly in AMD64 assembly, but in the portable assembly language qasm developed by Bernstein [8]. The aim of qasm is to reduce
development time of assembly software by offering a unified syntax across different architectures and by assisting the assembly programmer with register allocation. Most importantly for us, one line in \texttt{qhasm} translates to exactly one assembly instruction. Also, \texttt{qhasm} guarantees that “register variables” are indeed kept in registers. Spilling to memory has to be done explicitly by the programmer.

**Verifying \texttt{qhasm} code.** The Curve25519 software we verified is publicly available as part of the SUPERCOP benchmarking framework [9], but does not include the \texttt{qhasm} source files, which we obtained from the authors. Our verification works on \texttt{qhasm} level. The obvious disadvantage is that we rely on the correctness of \texttt{qhasm} translation. The advantage of this approach is that we can easily adapt our approach to assembly software for other architectures.

4.2 The Boolector SMT solver

Boolector is an efficient SMT solver supporting the bit vector and array theory [17]. In cryptographic software, arithmetic in large finite fields requires hundreds of significant bits. Standard algorithms for linear (integer) arithmetic do not apply. Boolector reduces queries to instances of the Boolean satisfiability problem by bit blasting and is hence more suitable for our purposes.

Theory of arrays is also essential to the formalization of \texttt{qhasm} programs. In low-level programming languages such as \texttt{qhasm}, memory and pointers are indispensable. On the other hand, \texttt{qhasm} programs are finite. Sizes of program variables (including pointers) must be declared. Subsequently, each variable is of finite domain and, more importantly, the memory is finite. Since formal models of \texttt{qhasm} programs are necessarily finite, they are expressible in theories of bit vectors and arrays. Boolector therefore fits perfectly in this application.

4.3 The Coq proof assistant

The Coq proof assistant has been developed in INRIA for more than twenty years [15]. The tool is based on a higher-order logic called the Calculus of Inductive Construction and has lots of libraries for various theories. In contrast to model-theoretic tools such as Boolector, proof assistants are optimized for symbolic reasoning. For instance, the algebraic equation \((x + y)^2 = x^2 + 2xy + y^2\) can be verified by the Coq tactic \texttt{ring} instantaneously.

In this work, we use the Coq standard library \texttt{ZArith} to formalize the congruence relation modulo \(2^{255} - 19\). For non-linear modulo relations in \(F_{2^{255} - 19}\), Boolector may fail to verify in a handful of cases. We verify them with our formalization and simple rewrite tactics in Coq.

5 Methodology

We aim to verify the Montgomery ladder step of the record-holding implementation of Curve25519 in [11,12]. A ladder step (Alg. 2) consists of 18 field arithmetic operations. Considering the complexity of a \(F_p\) multiplication (Sec. 3), the correctness of manually optimized \texttt{qhasm} implementation for the Montgomery ladder step is by no mean clear. Due to space limit, we only detail the verification of \(F_p\) multiplication. Other field arithmetic and the Montgomery ladder step (Alg. 2) itself are handled similarly.

We will use Hoare triples to specify properties about \texttt{qhasm} implementations. Let \(Q, Q'\) be predicate logic formulae, and \(P\) a \texttt{qhasm} program fragment. Informally, a Hoare triple
\( (Q) \mid P \mid (Q') \) specifies that the qasm fragment \( P \) ends in a state satisfying \( Q' \) provided that \( P \) starts in a state satisfying \( Q \). The formula \( Q \) and \( Q' \) are called pre- and post-conditions respectively. We only use quantifier-free pre- and post-conditions. The typewriter and Fraktur fonts are used to denote program and logical variables respectively in pre- and post-conditions.

Let \( P \) be a qasm implementation for \( \mathbb{F}_p \) multiplication. Note that \( P \) is loop-free. When the pre- and post-conditions are quantifier-free, it is straightforward to translate a Hoare triple \( (Q) \mid P \mid (Q') \) to a Boolector specification. We first convert the qasm fragment \( P \) into static single assignment form \( P_{\text{SSA}} \), and then check whether the quantifier-free formula \( Q \land P_{\text{SSA}} \land \neg Q' \) in the bit-vector theory is satisfiable. If not, we have established \( \models (Q) \mid P \mid (Q') \).

In order to automate this process, we have defined a simple assertion language to specify pre- and post-conditions in qasm. Moreover, we have build a converter that translates annotated qasm fragments into Boolector specifications.

### 5.1 \( \mathbb{F}_p \) multiplication in the radix-\( 2^{64} \) representation

Let \( P_{64} \) denote the qasm program for \( \mathbb{F}_p \) multiplication in the radix-\( 2^{64} \) representation. The inputs \( X = x_0 + 2^{64}x_1 + 2^{128}x_2 + 2^{192}x_3 \) and \( Y = y_0 + 2^{64}y_1 + 2^{128}y_2 + 2^{192}y_3 \) are stored in memory pointed to by the qasm variables \( xp \) and \( yp \) respectively. qasm uses a C-like syntax. Pointer dereferences, pointer arithmetic, and type coercion are allowed in qasm expressions. Thus, the limbs \( x_i \) and \( y_i \) correspond to the qasm expressions \(*(\text{uint64 } *)(xp + 8i)\) and \(*(\text{uint64 } *)(yp + 8i)\) respectively for every \( i \in [0, 3] \). We introduce logical variables \( r_i \) and \( \eta_i \) to record the limbs \( x_i \) and \( y_i \) respectively. Consider

\[
Q_{64_{xy,\text{eqns}}} := \bigwedge_{i=0}^{3} f_i^{64} = *(\text{uint64 } *)(xp + 8i) \land \bigwedge_{i=0}^{3} \eta_i^{64} = *(\text{uint64 } *)(yp + 8i)
\]

The operator \( \equiv \) denotes the \( n \)-bit equality in the theory of bit-vectors. The formula \( Q_{64_{xy,\text{eqns}}} \) states that the values of the logical variables \( r_i \) and \( \eta_i \) are equal to the limbs \( x_i \) and \( y_i \) of the initial inputs respectively.

In \( P_{64} \), the outcome is stored in memory pointed to by the qasm variable \( rp \). That is, the limb \( r_i \) of \( R = r_0 + 2^{64}r_1 + 2^{128}r_2 + 2^{192}r_3 \) corresponds to the qasm expressions \(*(\text{uint64 } *)(rp + 8i)\) for every \( i \in [0, 3] \). Define

\[
Q_{64_{r,\text{eqns}}} := \bigwedge_{i=0}^{3} r_i^{64} = *(\text{uint64 } *)(rp + 8i)
\]

\[
Q_{64_{\text{prod}}} := (\sum_{i=0}^{3} r_i 2^{64i}) \times (\sum_{i=0}^{3} \eta_i 2^{64i}) \equiv \sum_{i=0}^{512} r_i 2^{64i} \pmod{p}
\]

The operator \( \equiv \) denotes the \( n \)-bit signed modulo operator in the bit-vector theory. The formula \( Q_{64_{r,\text{eqns}}} \) introduces the logical variable \( r_i \) equal to the coefficient \( r_i \) for \( 0 \leq i \leq 3 \). The formula \( Q_{64_{\text{prod}}} \) specifies that the outcome \( R \) is indeed the product of \( X \) and \( Y \) in field arithmetic.

Consider the top-level Hoare triple \( (Q_{64_{xy,\text{eqns}}}) P_{64} (Q_{64_{r,\text{eqns}}} \land Q_{64_{\text{prod}}} \) \). We are concerned about the outcomes of the qasm fragment \( P_{64} \) from states where logical variables \( r_i \) and \( \eta_i \) are equal to limbs of the inputs pointed to by the program variables \( xp \) and \( yp \) respectively. During the execution of the qasm program \( P_{64} \), program variables may change their values. Logical variables, on the other hand, remain unchanged. The logical variables \( r_i \), \( \eta_i \) in the pre-condition \( Q_{64_{xy,\text{eqns}}} \) effectively memorize the input limbs before the execution of \( P_{64} \). The post-condition \( Q_{64_{r,\text{eqns}}} \land Q_{64_{\text{prod}}} \) furthermore specifies that the outcome pointed
For clarity, we introduce the logical variable $s$. The top-level Hoare triple specifies the multiply phase of $Q$ in the radix-2 representation.

The top-level Hoare triple contains complicated arithmetic operations over hundreds of 64-bit vectors. It is perhaps not unexpected that naive verification fails. In order to verify the $\text{qhasm}$ implementation of $F_p$ multiplication, we exploit the compositionality of proofs for sequential programs. Recall the proof rule for compositions in Hoare logic, where $Q'$ is a mid-condition:

\[
\vdash (Q) P_0 (Q) \vdash (Q') P_1 (Q'') \quad \text{Composition}
\]

Applying the proof rule, it suffices to find a mid-condition for the top-level Hoare triple. Recall that $F_p$ multiplication can be divided into two phases: multiply and reduce (Sec. 3.1). It is but natural to verify each phase separately. More precisely, we introduce logical variables to memorize values of program variables at start and end of each phase. The computation of each phase is thus specified by arithmetic relations between logical variables.

Multiply in the radix-$2^{64}$ representation Let $P_{64M}$ and $P_{64R}$ denote the $\text{qhasm}$ fragments for multiply and reduce respectively. The multiply fragment $P_{64M}$ computes the 512-bit value $S = (s_0, \ldots, s_7)$ in (1) stored in the memory pointed to by the $\text{qhasm}$ variable $sp$. Thus each 64-bit value $s_i$ corresponds to the $\text{qhasm}$ expression $*(\text{uint } 64 *) (sp + 8i)$ for every $i \in [0, 3]$. Define

\[
Q_{64,\text{eqns}} := \bigwedge_{i=0}^{7} s_i = *(\text{uint } 64 *) (sp + 8i) \\
Q_{64,\text{mult}} := A_0 = X_{0} \land A_1 = 2^{64} X_{1} + A_0 \land A_2 = 2^{128} X_{2} + A_1 \land \\
A_3 = 2^{192} X_{3} + A_2 \land X = \sum_{i=0}^{3} r_i 2^{64i} \land \sum_{i=0}^{7} s_i 2^{64i} = A_3
\]

For clarity, we introduce the logical variable $X$ for the input $X = x_0 + 2^{64} x_1 + 2^{128} x_2 + 2^{192} x_3$ in $Q_{64,\text{mult}}$. Consider the Hoare triple $(Q_{64,\text{eqns}}) P_{64M} (Q_{64,\text{eqns}} \land Q_{64,\text{mult}})$ The pre-condition $Q_{64,\text{eqns}}$ memorizes the limbs of the inputs $X$ and $Y$ in logical variables $r_i$'s and $y_i$'s. The formula $Q_{64,\text{eqns}}$ records the limbs $s_i$'s after the $\text{qhasm}$ fragment $P_{64M}$ in logical variables $s_i$'s. $Q_{64,\text{mult}}$ ensures that the limbs $s_i$'s are computed according to (1). In other words, the Hoare triple specifies the multiply phase of $F_p$ multiplication in the radix-$2^{64}$ representation.

Reduce in the radix-$2^{64}$ representation Following the reduction phase in Sec. 3.1, we introduce logical variables $s'_i$ and $s''_i$ for the limbs $s'_i$ and $s''_i$ respectively for every $i \in [0, 4]$. The formulæ $Q_{64,\text{red}}, Q_{64,\text{red}}, Q_{64,\text{red}}$ are defined for the three reduction steps. The formulæ $Q_{64,\text{red}}, Q_{64,\text{red}},$ and $Q_{64,\text{red}}$ moreover give upper bounds.
Proposition 1. Assume phase.

\[ s'_i \text{2}^{64i} = s_0 + 2^{64}s_1 + 2^{128}s_2 + 2^{192}s_3 + 38(s_4 + 2^{64}s_5 + 2^{128}s_6 + 2^{192}s_7) \]

\[ Q_{64_s'} \text{\_red} := \sum_{i=0}^{4} s'_i 2^{64i} = 320 \]

\[ Q_{64_{s'}} \text{\_bds} := \bigwedge_{i=0}^{4} 0 \leq s'_i < 2^{64} \]

\[ Q_{64_{s'}} \text{\_red} := \sum_{i=0}^{3} s'_i 2^{64i} = 38s'_4 + \sum_{i=0}^{3} s'_i 2^{64i} \]

\[ Q_{64_{s'}} \text{\_bds} := \bigwedge_{i=0}^{3} 0 \leq s''_i < 2 \land 0 \leq s''_i < 2 \]

\[ Q_{64_{r}} \text{\_red} := \sum_{i=0}^{3} r_i 2^{64i} = 38s'_4 + \sum_{i=0}^{3} s''_i 2^{64i} \]

\[ Q_{64_{r}} \text{\_bds} := \bigwedge_{i=0}^{3} 0 \leq r_i < 2^{64} \]

Consider the following Hoare triple

\[ (Q_{64_{\text{mult}}} P_{64_R} (Q_{64_{s'}} \text{\_red} \land Q_{64_{s'}} \text{\_bds} \land Q_{64_{s''}} \text{\_red} \land Q_{64_{s''}} \text{\_bds} \land)) \]

The pre-condition \( Q_{64_{\text{mult}}} \) assumes that variables \( s_i \)'s are obtained from the multiply phase. Recall the formula \( Q_{64_{r}} \text{\_eqns} \) defined at the beginning of this subsection. The post-condition states that outcome \( r_i \)'s are obtained by the reduce phase. Note that the logical variable \( s''_i \) for the limb \( s''_i \) is at most 1. We are using BOOLECTOR to verify this fact in the reduction phase.

**Proposition 1. Assume**

1. \( \models (Q_{64_{\text{eqns}}} P_{64_M} (Q_{64_{s}} \land Q_{64_{\text{mult}}})) \)
2. \( \models (Q_{64_{\text{mult}}} P_{64_R} (Q_{64_{s'}} \land Q_{64_{s'}} \land Q_{64_{s''}} \land Q_{64_{s''}} \land)) \)

Then \( \models (Q_{64_{\text{eqns}}} P_{64_M} P_{64_R} (Q_{64_{\text{red}}} \land Q_{64_{\text{bds}}} \land)) \).

Note that the Hoare triples in the proposition do not establish \( Q_{64_{\text{prod}}} \) directly. Indeed, we need to show

\[ Q_{64_{\text{mult}}} \land Q_{64_{s'}} \land Q_{64_{s'}} \land Q_{64_{s'}} \land Q_{64_{r}} \land Q_{64_{r}} \land Q_{64_{r}} \land Q_{64_{r}} \implies Q_{64_{\text{prod}}} \]

in the proof of Proposition 1. Observe that the statement involves modular operations in the bit-vector theory. Although the statement is expressible in a quantifier-free formula in the theory of bit-vectors, the SMT solver BOOLECTOR could not verify it. We therefore use the proof assistant COQ to formally prove the statement. With simple facts about modular arithmetic such as \( 38 \equiv 2^{56} \pmod{p} \), our formal COQ proof needs less than 800 lines.

### 5.2 \( \mathbb{F}_p \) multiplication in the radix-\( 2^{51} \) representation

Let \( P_{51} \) denote the qasm fragment for \( \mathbb{F}_p \) multiplication in radix-\( 2^{51} \) representation. The inputs \( X = x_0 + 2^{51}x_1 + 2^{102}x_2 + 2^{153}x_3 + 2^{204}x_4 \), \( Y = y_0 + 2^{51}y_1 + 2^{102}y_2 + 2^{153}y_3 + 2^{204}y_4 \), and outcome \( R = r_0 + 2^{51}r_1 + 2^{102}r_2 + 2^{153}r_3 + 2^{204}r_4 \) are stored in memory pointed to by the qasm variables \( x_0, y_0 \) and \( r_0 \) respectively. We thus introduce logical variables \( r_1, y_1, \text{and } r_1 \) to memorize the values of the qasm expressions \( *((\text{uint64 } *) ((x_0 + 8i)) \cdot y_0 + 8i) \), and \( *((\text{uint64 } *) ((x_0 + 8i)) \cdot r_0 + 8i) \) respectively for every \( i \in [0, 4] \).

The formulae \( Q_{51_{\text{eqns}}} \), \( Q_{51_{r}} \text{\_eqns} \), \( Q_{51_{\text{prod}}} \) are defined similarly as in the radix-\( 2^{64} \) representation. Observe that each limb in the radix-\( 2^{51} \) representation has only 51 significant bits.
The formulae $Q_{51_{xy,bds}}$ and $Q_{51_{r,bds}}$ specify that the inputs and outcome are in the radix-$2^{51}$ representation.

$$Q_{51_{xy,bds}} := \bigwedge_{i=0}^{4} 0 \leq r_i < 2^{51} \land \bigwedge_{i=0}^{4} 0 \leq \eta_i < 2^{51} \quad Q_{51_{r,bds}} := \bigwedge_{i=0}^{4} 0 \leq r_i < 2^{51}$$

In the top-level Hoare triple $(Q_{51_{xy,eqns} \land Q_{51_{xy,bds}}} \land P_{51}(Q_{51_{r,eqns} \land Q_{51_{r,bds}} \land Q_{51_{prod}}}))$, the pre-condition $Q_{51_{xy,eqns} \land Q_{51_{xy,bds}}}$ assumes that the inputs $X$ and $Y$ are in the radix-$2^{51}$ representation. The post-condition $Q_{51_{r,eqns} \land Q_{51_{r,bds}} \land Q_{51_{prod}}}$ specifies that the outcome is the product of $X$ and $Y$ in the radix-$2^{51}$ representation. The top-level Hoare triple hence specifies that the qhasm fragment $P_{51}$ is $\mathbb{F}_p$ multiplication in the radix-$2^{51}$ representation.

Similar to the case in the radix-$2^{128}$ representation, the top-level Hoare triple should be decomposed before verification. Recall that $\mathbb{F}_p$ multiplication in the radix-$2^{51}$ representation has two phases: multiply-and-reduce and delayed carry (Sec. 3.2). We therefore verify each phase separately.

Let $P_{51_{MR}}$ and $P_{51_D}$ denote the qhasm fragment for multiply-and-reduce and delayed carry respectively. In the multiply-and-reduce phase, the qhasm fragment $P_{51_{MR}}$ computes $s_i$'s in (2). Since each $s_i$ has 128 significant bits, $P_{51_{MR}}$ actually stores each $s_i$ in a pair of 64-bit qhasm variables $s_i.l$ and $s_i.h$. We will use the qhasm expression $u.v$ to denote $u \times 2^{64} + v$. Define

$$Q_{51_{r,eqns}} := \bigwedge_{i=0}^{4} s_i^{128} = s_i.h.s_i.l$$

$$Q_{51_{mult_red}} := s_0^{128} = (f_0\eta_0 + 19(f_1\eta_4 + f_2\eta_3 + f_3\eta_2 + f_4\eta_1)) \land$$

$$s_1^{128} = (f_0\eta_1 + f_1\eta_0 + 19(f_2\eta_4 + f_3\eta_3 + f_4\eta_2)) \land$$

$$s_2^{128} = (f_0\eta_2 + f_1\eta_1 + f_2\eta_0 + 19(f_3\eta_4 + f_4\eta_3)) \land$$

$$s_3^{128} = (f_0\eta_3 + f_1\eta_2 + f_2\eta_1 + f_3\eta_0 + 19f_4\eta_4) \land$$

$$s_4^{128} = (f_0\eta_4 + f_1\eta_3 + f_2\eta_2 + f_3\eta_1 + f_4\eta_0).$$

$Q_{51_{r,eqns}}$ states that the logical variable $s_i$ is equal to the qhasm expression $s_i.h.s_i.l$ for every $i \in [0, 4]$. $Q_{51_{mult_red}}$ specifies that $s_i$ are computed correctly for every $i \in [0, 4]$. Nonetheless, we find the condition $Q_{51_{mult_red}}$ is too weak to prove the correctness of the multiply-and-reduce phase. If $s_i.h.s_i.l$ indeed had 128 significant bits, overflow could occur during bitwise operations in multiply-and-reduce. To verify multiplication, we estimate tighter upper bounds for $s_i$’s.

Recall that $s_i$’s are sums of products of $x_i$’s and $y_j$’s which are bounded by $2^{51}$. A simple computation gives us better upper bounds for $s_i$’s. Define

$$Q_{51_{s,bds}} := 0 \leq s_0 \leq 2^{102} + 4 \cdot 19 \cdot 2^{102} \land 0 \leq s_1 \leq 2 \cdot 2^{102} + 3 \cdot 19 \cdot 2^{102} \land$$

$$0 \leq s_2 \leq 3 \cdot 2^{102} + 2 \cdot 19 \cdot 2^{102} \land 0 \leq s_3 \leq 4 \cdot 2^{102} + 19 \cdot 2^{102} \land$$

$$0 \leq s_4 \leq 5 \cdot 2^{102}$$

Consider the Hoare triple $(Q_{51_{xy,eqns} \land Q_{51_{xy,bds}}} \land P_{51_{MR}}(Q_{51_{r,eqns} \land Q_{51_{s,bds}} \land Q_{51_{mult_red}}}))$, in addition to checking whether qhasm variables $s_i.h$’s and $s_i.l$’s are computed correctly, the qhasm fragment $P_{51_{MR}}$ for multiply-reduce is required to meet the upper bounds in $Q_{51_{s,bds}}$. The mid-condition $Q_{51_{s,bds}} \land Q_{51_{mult_red}}$ enables the verification of the qhasm fragment $P_{51_D}$ for the delayed carry phase.
The \texttt{qasm} fragment $P_{51D}$ for delayed carry performs carrying on 128-bit expressions $s_i, t_i, 1$’s to obtain the product of the inputs $X$ and $Y$. The product must also be in the radix-$2^{51}$ representation. Define

$$Q_{51\text{delayed\_carry}} := \sum_{i=0}^{4} s_i 2^{51i} \equiv \sum_{i=0}^{4} t_i 2^{51i} \pmod{p}.$$  

The Hoare triple $\langle Q_{51\text{\_eqns}} \land Q_{51\text{\_bds}} \land Q_{51\text{\_mult\_red}} \rangle P_{51D} \langle Q_{51\text{\_delayed\_carry}} \land Q_{51\text{\_r\_bds}} \rangle$ verifies that the \texttt{qasm} fragment $P_{51D}$ computes a number $\sum_{i=0}^{4} t_i 2^{51i}$ in the radix-$2^{51}$ representation, and it is congruent to $\sum_{i=0}^{4} s_i 2^{51i}$ modulo $p$.

**Proposition 2.** Assume

1. $\models \langle Q_{51\text{\_eqns}} \land Q_{51\text{\_bds}} \land Q_{51\text{\_mult\_red}} \rangle P_{51MR} \langle Q_{51\text{\_eqns}} \land Q_{51\text{\_bds}} \land Q_{51\text{\_mult\_red}} \rangle$;
2. $\models \langle Q_{51\text{\_eqns}} \land Q_{51\text{\_bds}} \land Q_{51\text{\_mult\_red}} \rangle P_{51D} \langle Q_{51\text{\_delayed\_carry}} \land Q_{51\text{\_r\_bds}} \rangle$.

Then $\models \langle Q_{51\text{\_eqns}} \land Q_{51\text{\_bds}} \rangle P_{51D}; P_{51D} \langle Q_{51\text{\_prod}} \land Q_{51\text{\_r\_bds}} \rangle$.

The Hoare triples in the proposition do not establish $Q_{51\text{\_prod}}$ directly. Again, we formally show $\vdash [Q_{51\text{\_bds}} \land Q_{51\text{\_mult\_red}} \land Q_{51\text{\_delayed\_carry}}] \implies Q_{51\text{\_prod}}$ in the proof assistant Coq. Our Coq proof contains less than 600 lines.

The verification of the Montgomery ladder step (Alg. 2) is carried out after all field arithmetic operations are verified separately. We replace fragments for field arithmetic by their corresponding pre- and post-conditions. Alg. 2 is then converted to the static single assignment form. We then assert the static single assignments as the post-condition of Alg. 2. UsingBoolector, we verify that the post-condition holds, and that the post-condition of every field operation implies the pre-condition of the following field operation in Alg. 2. The record-holding implementation for the Montgomery ladder step in the radix-$2^{51}$ and radix-$2^{64}$ representations are formally verified.

### 6 Results and Discussion

In this section, we present results and findings during the verification process. A summary of the experimental results is in Table 1. The columns are the number of limbs, the number of mid-conditions used, and the verification time used in Boolector. We run Boolector 1.6.0 on a Linux machine with 3.07-GHz CPU and 32-GB memory. We did not set a timeout and thus a verification task can run until it is killed by the operating system.

We formally verified the ladder step in Algorithm 2 in both radix-$2^{64}$ and radix-$2^{51}$. The pre and postconditions of each operators are obtained from the verification of the corresponding \texttt{qasm} code \texttt{fe25519r64\_star/fe25519\_star}. We are able to reproduce a known bug in an old version of \texttt{F2\_255\_19} multiplication (\texttt{fe25519r64\_mul-1}). A counterexample can be found in seconds with a pair of precondition and postcondition for the reduction phase. The rows mul25519-p2-1 and mul25519-p2-2 are the results of verifying the delayed carry phase of mul25519, a 3-phase implementation of a multiplication. The result shows that if we add an additional mid-condition to the delayed carry phase of mul25519, the verification time of the delayed carry phase can be reduced from 2723 minutes to 263 minutes.
Note that all post-conditions for the radix-$2^{64}$ are equalities. Since BOOLECTOR cannot verify modular congruence relations in the radix-$2^{64}$ representation, we have to establish them in Coq. On the other hand, BOOLECTOR successfully verifies the modular congruence relation $Q51_{\text{delay/carry}}$ for the radix-$2^{51}$ representation. Our Coq proof for the radix-$2^{51}$ representation is thus simplified. The reason why some congruence relations is verified in the radix-$2^{51}$ representation is because we are able to divide $P51_P$ further into smaller fragments. A few extra carry bits can not only reduce the time for execution but also verification.

We found the following heuristics are quite useful to accelerate verification. We cannot verify many of the cases without them. First, we split conjuncted postconditions, i.e., translate $\langle Q0 \rangle P(Q1 \land Q2)$ to $\langle Q0 \rangle P(Q1)$ and $\langle Q0 \rangle P(Q2)$. This reduces the verification time of the multiply phase of $\text{mul25519}$ from one day to one minute. Second, we delay bit-width extension. For example, consider a formula $a \equiv b \times c$ where $a$ has 256 bits and $b, c$ have 64 bits. Instead of extending $b$ and $c$ to 256 bits before the multiplication, we first extend $b$ and $c$ to 128 bits, compute the multiplication, and then extend the result to 256 bits. Third, we over-approximate BOOLECTOR specifications automatically by reducing logical variables and weakening preconditions. The validity of an over-approximated specification guaranteed the validity of the original one, but not vice versa. To be more specific, given a specification $\langle Q1 \rangle P \langle Q1 \rangle Q1 \land \cdots \land Q_n P(Q_n)$, our translator automatically removes logical variables that do not appear in $Q1$; it removes $Q_i$ if some variable in $Q_i$ neither appears in $Q1$ nor gets updated in $P$. We cannot verify $\text{fe25519r64_sq}$ and $\text{fe25519_sq}$ without this heuristic.

### 7 Future work

There are several avenues for future work. One interesting topic could be to develop verification approaches for ensuring that the an assembly implementation is resistant against side-channel attacks. Formal techniques in measuring worst case execution time (WCET) might be a starting point for this line of research.

Currently, we need to manually provide mid-conditions for verifications. Although the verification steps between preconditions and postconditions are done automatically, it would be even better if we can increase the degree of automation further by investigating techniques.
for automatic insertion of mid-conditions. We think the tools for automatic assertion insertion could be relevant [21]. The tool obtain assertions based on given templates of assertions and by synthesizing them dynamically from observed executions traces.

Our translator currently can produce BOOLECTOR specifications from annotated qhasm files. Recall that some properties that cannot be proved in BOOLECTOR are proved in Coq. It would be good if the translator can produce both BOOLECTOR specifications and Coq proof obligations from an annotated qhasm file, which makes the qhasm file more self-contained. Moreover, tactics of Coq may be developed to solve some specific problems, for example, modular congruence, to reduce human work.

References


32. Tor project: Anonymity online. [https://www.torproject.org/](https://www.torproject.org/).