CryptoLine

January 15, 2022

1 Introduction

CryptoLine is a tool and a language for the verification of low-level implementations of mathematical constructs. In CryptoLine, users can specify two kinds of properties, namely algebraic properties and range properties. Algebraic properties involve equalities and modular equalities in the integer domain while range properties involve bit-accurate variable ranges. CryptoLine verifies algebraic properties and range properties separately. Verification of algebraic properties is reduced to ideal membership queries which are solved by external computer algebra systems. Verification of range properties is reduced to Satisfiability Modulo Theories (SMT) queries which are solved by external SMT solvers.

2 CryptoLine Language

A Syntax of CryptoLine

An *identifier* is a regular string started by a letter or an underscore, followed by letters, digits, or underscores.

$$id ::= (letter \mid underscore)[letter \mid digit \mid underscore]$$

All constants and variables in CryptoLine are typed. Let w be a positive integer. uint$w$ and sint$w$ in CryptoLine denote the types of bit-vectors with width w in the unsigned and two's complement signed representations respectively. The type uint1 is also written as bit.

$$typ \quad ::= \quad \mathsf{uint1} \mid \mathsf{sint2} \mid \mathsf{uint2} \mid \mathsf{sint3} \mid \cdots \mid \mathsf{uint}w \mid \mathsf{sint}(w+1)$$

A *constant* is an integer, a hexadecimal number, a named constant, or arithmetic expressions over constants.

$$
\begin{array}{rcl}
\mathit{const} & ::= & \mathit{simple\_const} \\
& | & \textbf{(}\ \mathit{complexy\_const}\ \textbf{)} \\
\mathit{simple\_const} & ::= & \mathbb{Z} \\
& | & 0x[0-9a-fA-F]^{+} \\
& | & \$\mathit{id} \\
\mathit{complexy\_const} & ::= & \mathit{const} \\
& | & \textbf{-}\ \mathit{complexy\_const} \\
& | & \mathit{complexy\_const}\ \textbf{+}\ \mathit{complexy\_const} \\
& | & \mathit{complexy\_const}\ \textbf{-}\ \mathit{complexy\_const} \\
& | & \mathit{complexy\_const}\ \textbf{*}\ \mathit{complexy\_const} \\
& | & \mathit{complexy\_const}\ \textbf{**}\ \mathit{complexy\_const} \\
\mathit{typed\_const} & ::= & \mathit{const}@\mathit{typ} \\
& | & \mathit{typ}\ \mathit{const}
\end{array}
$$

The value of a named integer c is read by $\$c$. CRYPTOLINE supports the following arithmetic operators over constants: unary minus (-), addition (+), subtraction (-), multiplication (*), and exponent (**). A *typed constant* is a constant with its type explicitly specified.

A *variable* is an identity. A *typed variable* is a variable with its type explicitly specified. An *lval* is either a variable or a typed variable.

$$
\begin{array}{rcl}
\mathit{var} & ::= & \mathit{id} \\
\mathit{typed\_var} & ::= & \mathit{var}@\mathit{typ} \mid \mathit{typ}\ \mathit{var} \\
\mathit{lval} & ::= & \mathit{var} \mid \mathit{typed\_var}
\end{array}
$$

The notation $t^*_\circ$ and $t^+_\circ$ respectlvey represents a possibly empty and a non-empty sequence of $\circ$-separated t.

An *atom* is either a typed constant, a variable, or a typed variable. It is not necessary to specify the variable type explicitly in an atom because CRYPTOLINE can infer the type automatically.

$$\mathit{atom} ::= \mathit{typed\_const} \mid \mathit{var} \mid \mathit{typed\_var}$$

An *algebraic expression* is evaluated over $\mathbb{Z}$.

$$
\begin{array}{rclcl}
\mathit{eexp} & ::= & \mathit{simple\_const} & | & \mathit{var} \\
& | & \textbf{-}\ \mathit{eexp} & | & \mathit{eexp}\ \textbf{+}\ \mathit{eexp} \\
& | & \mathit{eexp}\ \textbf{-}\ \mathit{eexp} & | & \mathit{eexp}\ \textbf{*}\ \mathit{eexp} \\
& | & \mathit{eexp}\ \textbf{**}\ \mathit{eexp} & | & \textbf{\textit{limbs}}\ \mathit{const}\ \textbf{[}\ \mathit{eexp}^{+}_{,}\ \textbf{]} \\
& | & \textbf{(}\ \mathit{eexp}\ \textbf{)} & &
\end{array}
$$

limbs $n\,[e_1, \ldots, e_m]$ represents $e_1 + e_2 2^n + e_3 2^{2n} + \cdots + e_m 2^{mn}$. A *range expression* is evaluated over bit vectors. *const* w n is a bit-vector of width w and value n. $\sim$ (*neg*) is logical negation. ! (*not*), & (*and*), | (*or*), ^ (*xor*) are respectively bit-wise negation, bit-wise AND, bit-wise OR, and bit-wise XOR. *umod* is unsigned remainder. *srem* is 2's complement signed remainder (sign follows dividend).

smod is 2's complement signed remainder (sign follows divisor). *uext* and *sext* are respectively unsigned and signed extension operations.

$$
\begin{array}{rclcl}
\mathit{rexp} & ::= & \texttt{(}\ \mathit{rexp}\ \texttt{)} & \mid & \textbf{\textit{const}}\ \mathit{const}\ \mathit{const} \\
& \mid & \texttt{-}\ \mathit{rexp} & \mid & \mathit{rexp}\ \texttt{+}\ \mathit{rexp} \\
& \mid & \mathit{rexp}\ \texttt{-}\ \mathit{rexp} & \mid & \mathit{rexp}\ \texttt{*}\ \mathit{rexp} \\
& \mid & \texttt{\~{}}\ \mathit{rexp} & \mid & \textbf{\textit{neg}}\ \mathit{rexp} \\
& \mid & \texttt{!}\ \mathit{rexp} & \mid & \textbf{\textit{not}}\ \mathit{rexp} \\
& \mid & \mathit{rexp}\ \texttt{\&}\ \mathit{rexp} & \mid & \textbf{\textit{and}}\ \mathit{rexp}\ \mathit{rexp} \\
& \mid & \mathit{rexp}\ \texttt{|}\ \mathit{rexp} & \mid & \textbf{\textit{or}}\ \mathit{rexp}\ \mathit{rexp} \\
& \mid & \mathit{rexp}\ \texttt{\^{}}\ \mathit{rexp} & \mid & \textbf{\textit{xor}}\ \mathit{rexp}\ \mathit{rexp} \\
& \mid & \textbf{\textit{umod}}\ \mathit{rexp}\ \mathit{rexp} & \mid & \textbf{\textit{srem}}\ \mathit{rexp}\ \mathit{rexp} \\
& \mid & \textbf{\textit{smod}}\ \mathit{rexp}\ \mathit{rexp} & \mid & \textbf{\textit{limbs}}\ \mathit{const}\ \texttt{[}\ \mathit{rexp}^{+}_{,}\ \texttt{]} \\
& \mid & \textbf{\textit{uext}}\ \mathit{rexp}\ \mathit{const} & \mid & \textbf{\textit{sext}}\ \mathit{rexp}\ \mathit{const}
\end{array}
$$

A *predicate* is represented by an algebraic predicate and a range predicate.

$$
\mathit{pred} \ ::= \ \textbf{\textit{true}} \ \mid \ \mathit{epred}\ \texttt{\&\&}\ \mathit{rpred}
$$

An *algebraic predicate* is evaluated over the integer domain. $e_1 = e_2$ $(eq\ e_1\ e_2)$ is an equality over algebraic expressions. $e_1 = e_2\ (mod\ e_3)$ $(eqmod\ e_1\ e_2\ e_3)$ is a modular equality. p_1 /\ p_2 $(and\ p_1\ p_2)$ is a logical conjunction of p_1 and p_2. The conjunction of a sequence of algebraic predicates $e_1, \ldots, e_n$ is written as /\ $[e_1, \ldots, e_n]$ $(and\ [e_1, \ldots, e_n])$.

$$
\begin{array}{rclcl}
\mathit{epred} & ::= & \texttt{(}\ \mathit{epred}\ \texttt{)} & \mid & \textbf{\textit{true}} \\
& \mid & \mathit{eexp}\ \texttt{=}\ \mathit{eexp} & \mid & \textbf{\textit{eq}}\ \mathit{eexp}\ \mathit{eexp} \\
& \mid & \mathit{eexp}\ \texttt{=}\ \mathit{eexp}\ \texttt{(}\ \textbf{mod}\ \mathit{eexp}\ \texttt{)} & \mid & \textbf{\textit{eqmod}}\ \mathit{eexp}\ \mathit{eexp}\ \mathit{eexp} \\
& \mid & \mathit{epred}\ \texttt{/\textbackslash}\ \mathit{epred} & \mid & \textbf{\textit{and}}\ \mathit{epred}\ \mathit{epred} \\
& \mid & \texttt{/\textbackslash}\ \texttt{[}\ \mathit{epred}^{+}_{,}\ \texttt{]} & \mid & \textbf{\textit{and}}\ \texttt{[}\ \mathit{epred}^{+}_{,}\ \texttt{]}
\end{array}
$$

A *range predicate* specifies the ranges of variables. CryptoLine offers comparisons such as equality (=), modular equalities (*equmod*, *eqsmod*, *eqsrem*), unsigned less than (<), unsigned less than or equal to (<=), unsigned greater than (>), unsigned greater than or equal to (>=), signed less than (< s), signed less than or equal to (<= s), signed greater than (> s), and signed greater than or equal to ($>= s$).

$$
\begin{array}{lcl|l}
\mathit{rpred} & ::= & (\ \mathit{rpred}\ ) & \textit{\textbf{true}} \\
 & | & \mathit{rexp}\ =\ \mathit{rexp} & \textit{\textbf{eq}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ =\ \mathit{rexp}\ (\ \mathit{umod}\ \mathit{rexp}\ ) & \textit{\textbf{equmod}}\ \mathit{rexp}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ =\ \mathit{rexp}\ (\ \mathit{smod}\ \mathit{rexp}\ ) & \textit{\textbf{eqsmod}}\ \mathit{rexp}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ =\ \mathit{rexp}\ (\ \mathit{srem}\ \mathit{rexp}\ ) & \textit{\textbf{eqsrem}}\ \mathit{rexp}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ <\ \mathit{rexp} & \textit{\textbf{ult}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ <=\ \mathit{rexp} & \textit{\textbf{ule}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ >\ \mathit{rexp} & \textit{\textbf{ugt}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ >=\ \mathit{rexp} & \textit{\textbf{uge}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ <\textit{\textbf{s}}\ \mathit{rexp} & \textit{\textbf{slt}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ <=\textit{\textbf{s}}\ \mathit{rexp} & \textit{\textbf{sle}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ >\textit{\textbf{s}}\ \mathit{rexp} & \textit{\textbf{sgt}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \mathit{rexp}\ >=\textit{\textbf{s}}\ \mathit{rexp} & \textit{\textbf{sge}}\ \mathit{rexp}\ \mathit{rexp} \\
 & | & \sim\ \mathit{rpred} & \textit{\textbf{neg}}\,\mathit{rpred} \\
 & | & \mathit{rpred}\ /\backslash\ \mathit{rpred} & \textit{\textbf{and}}\ \mathit{rpred}\ \mathit{rpred} \\
 & | & \mathit{rpred}\ \backslash/\ \mathit{rpred} & \textit{\textbf{or}}\ \mathit{rpred}\ \mathit{rpred} \\
 & | & /\backslash\ [\ \mathit{rpred}^{+}_{,}\ ] & \textit{\textbf{and}}\ [\ \mathit{rpred}^{+}_{,}\ ] \\
 & | & \backslash/\ [\ \mathit{rpred}^{+}_{,}\ ] & \textit{\textbf{or}}\ [\ \mathit{rpred}^{+}_{,}\ ]
\end{array}
$$

There are numerous *instructions* supported by CryptoLine. *mov* x a assigns destination variable x by the value of the source atom a. *cmov* x c a_1 a_2 assigns destination variable x by the value of the source atom a_1 if the condition bit c is 1, and otherwise by the value of the source atom a_2. *add* x a_1 a_2 assigns x by the addition of the source atoms a_1 and a_2. Note that *add* may overflow. *adds* c x a_1 a_2 assigns x by the addition of the source atoms a_1 and a_2 with carry bit c set. *addr* c x a_1 a_2 assigns x by the addition of the source atoms a_1 and a_2 with carry bit c reset to 0. *adc* x a_1 $a_2 y$ assigns x by the addition of the carry bit y and the source atoms a_1 and a_2. *adcs* and *adcr* are the same as *adc* except the carry bit is respectively set and reset. There are also instructions *sub* for subtraction; *subc*, *sbc* and *isbcs* for subtraction with carry; *subb*, *sbb*, and *sbbs* for subtraction with borrow. *mul*, *muls*, and *mulr* are half multiplication operations. The differenace is that *muls* sets the carry bit if the multiplication under- or over-flow while *mulr* always resets the carry bit. *mull* is full multiplication with results split into high part and low part. *mulj* is also full multiplication without splitting the results. *set* x assigns the bit variable x by 1 while *clear* x assigns the bit variable x by 0. *and*, *or*, *not*, and *xor* are bit-wise operations. *assert* tells CryptoLine to verify the specified predicate. *assume* tells CryptoLine to assume the specified predicate. *cut* e && r is an alias of one *ecut* e followed by a *rcut* r. For *ecut*, CryptoLine verifies the specified algebraic predicate and starts afresh with the predicate assumed when verifying algebraic properties. Similarly for *rcut*, CryptoLine verifies the specified range predicate and starts afresh with the predicate assumed when verifying range properties. *call* p $(a_1, a_2, \ldots, a_n)$ executes a defined procedure

p with arguments $a_1, a_2, \ldots, a_n$.

$$
\begin{array}{lcll}
\mathit{instr} & ::= & \mathbf{mov}\ \mathit{lval}\ \mathit{atom} & \mid\ \mathbf{cmov}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{add}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{adds}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{addr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{adc}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} \\
& \mid & \mathbf{adcs}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} & \mid\ \mathbf{adcr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} \\
& \mid & \mathbf{sub}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{subc}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{subb}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{subr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{sbc}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} & \mid\ \mathbf{sbcs}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} \\
& \mid & \mathbf{sbcr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} & \mid\ \mathbf{sbb}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} \\
& \mid & \mathbf{sbbs}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} & \mid\ \mathbf{sbbr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{var} \\
& \mid & \mathbf{mul}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{muls}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{mulr}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{mull}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{mulj}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{nondet}\ \mathit{lval} \\
& \mid & \mathbf{set}\ \mathit{lval} & \mid\ \mathbf{clear}\ \mathit{lval} \\
& \mid & \mathbf{shl}\ \mathit{lval}\ \mathit{atom}\ \mathit{const} & \mid\ \mathbf{cshl}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom}\ \mathit{const} \\
& \mid & \mathbf{split}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{const} & \mid\ \mathbf{join}\ \mathit{lval}\ \mathit{lval}\ \mathit{atom}\ \mathit{const} \\
& \mid & \mathbf{and}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} & \mid\ \mathbf{or}\ \mathit{lval}\ \mathit{atom}\ \mathit{atom} \\
& \mid & \mathbf{xor}\ \mathit{lval}\ \mathit{atomatom} & \mid\ \mathbf{not}\ \mathit{lval}\ \mathit{atom} \\
& \mid & \mathbf{assert}\ \mathit{pred} & \mid\ \mathbf{assume}\ \mathit{pred} \\
& \mid & \mathbf{cut}\ \mathit{pred\_clause} & \mid\ \mathbf{ecut}\ \mathit{epred\_clause} \\
& \mid & \mathbf{rcut}\ \mathit{rpred\_clause} & \mid\ \mathbf{ghost}\ \mathit{typed\_var}^{+}_{,}\ \mathbf{:}\ \mathit{pred} \\
& \mid & \mathbf{call}\ \mathit{id}\ \mathbf{(}\ \mathit{atom}^{*}_{,}\ \mathbf{)} & \mid\ \mathbf{nop}
\end{array}
$$

Instructions *add*, *adds*, *addr*, *adc*, *adcs*, *adcr*, *sub*, *subc*, *subb*, *subr*, *sbc*, *sbcs*, *sbcr*, *sbb*, *sbbs*, *sbbr*, *mul*, *muls*, *mulr*, *mull*, *mulj*, and *split* also have specific unsigned and signed versions with prefix “u” or “s”. For example, *uadd* and *sadd* are respectively unsigned and signed versions of *add*.

Sometimes a predicate has to be proved with facts that have been cut off. CryptoLine offers the specification of hints required to prove a predicate.

$$
\begin{array}{rcll}
\mathit{pred\_clause} & ::= & \mathit{true} & \mid\ \mathit{epred\_clause}\ \mathbf{\&\&}\ \mathit{rpred\_clause} \\
\mathit{epred\_clause} & ::= & \mathit{epred} & \mid\ \mathit{epred}\ \mathbf{prove\ with}\ [\mathit{prove\_with}^{+}_{,}] \\
& \mid & \mathit{epred\_clause}^{+}_{,} & \\
\mathit{rpred\_clause} & ::= & \mathit{rpred} & \mid\ \mathit{rpred}\ \mathbf{prove\ with}\ [\mathit{prove\_with}^{+}_{,}] \\
& \mid & \mathit{rpred\_clause}^{+}_{,} & \\
\mathit{prove\_with} & ::= & \mathbf{precondition} & \mid\ \mathbf{all\ cuts} \\
& \mid & \mathbf{all\ assumes} & \mid\ \mathbf{all\ ghosts} \\
& \mid & \mathbf{cuts}\ [\mathbb{N}^{+}_{,}] &
\end{array}
$$

Note that the indices of *ecut* and *rcut* are numbered separately (starting from 0). When verifying algebraic properties, *rcut* instructions are ignored. When verifying range properties, *ecut* instructions are ignored. For example, consider the following program.

```
mov x 15@uint16;
ecut x = 15;
```

```
mov y 3@uint16;
cut y = 3 && and [x = 15@16, y = 3@16];
add z x y;
rcut z = 18@16;
```

If we want to prove e *prove_with* $[cuts[1]]$ && r *prove_with* $[cuts[1]]$, then $y = 3$ will be assumed when proving the algebraic property e while $z = 18@16$ will be assumed when proving the range property r.

A *procedure* is a parameterized program together with its specification (precondition and postcondition).

$$proc ::= \textbf{proc}\ id\ \textbf{(}\ formals\ \textbf{)} = \textbf{\{}\ pre\ \textbf{\}}\ prog\ \textbf{\{}\ post\ \textbf{\}}$$

The *formal parameters* of a procedure may be separated by a semicolon into *inout* and *out* variables.

$$formals ::= typed\_var^*_, \mid typed\_var^*_,\ \textbf{;}\ typed\_var^*_,$$

Variables before the semicolon are inout variables while variables after the semicolon are out variables. Formal parameters without a semicolon are all inout variables. The difference between inout and out variables is that when calling a procedure, actual parameters of the inout formal variables must be defined but this is not required for the actual parameters of the out formal variables. However, this does not mean that an out variable can be read before initialized. Every variable must be initialized before reading its value. A *precondition* is a predicate.

$$pre ::= pred$$

A *postcondition* is a predicate clause.

$$post ::= pred\_clause$$

A *statement* is a declaration of a procedure or a named integer.

$$stmt \quad ::= \quad proc \quad \mid \quad \textbf{const}\ id\ \textbf{=}\ const$$

A *program* is a sequence of semicolon separated statements. The entry point of the program is the *main* procedure. Other procedures called in main are inlined.

$$prog ::= stmt^+_;$$