CLIP: A Cryptographic Language with Irritating Parentheses

Yi-Hsiu Chen(yc2796)
Wei Duan(wd2214)

Introduction

- Motivation
  - Cryptographers
- Language features
  - Functional (Lisp)
  - Big number (GMP)
  - Bit sequence
- Cryptosystem
  - Public Key (RSA, El Gamel...)
  - Private Key (AES...)

Language Tutorial

(defvar|defun|expression)*

```
defvar i:int = 5;

defvar bs:bit#7 = ‘1011010;

defvar s:string = “Hello World”;

defvar n:int[2][3] = {{1 2 4} {3 5 7}};

defun square:int n:int =  (* n n);

 (+ (square 3) 2)
```

Built-in function

For big number

+, -, *, /, mod, pow, inverse, is-prime, next-prime

For bits number

zero, rand, pad, flip, flip-bit

For vector operation

group, merge, make-vector, transpose

For logic operation

and, or, not, ^(xor)

For comparison operation

less, greater, leq, geq, eq, neq, and, or, not

For conversion

int-of-bits, bits-of-int, string-of-bits, bits-of-string

Miscellaneous

let, map, reduce, lambda

Example Program

```
defun gcd:int a:int b:int=
(if (eq a b)
    a
    (if (greater a b)
        (gcd (- a b) b)
        (gcd a (- b a)))));
```

(gcd 5 15) ~~ Print 5

Example Program

```
defun theta:bit#64[5][5] block:bit#64[5][5] =
(let <col-par:bit#320 (reduce ^ (map merge block))>
     (map (lambda <row:bit#320>
          (group (^ row (>>> col-par 64) (<<< col-par 63)) 64))
          (map merge block)));
```

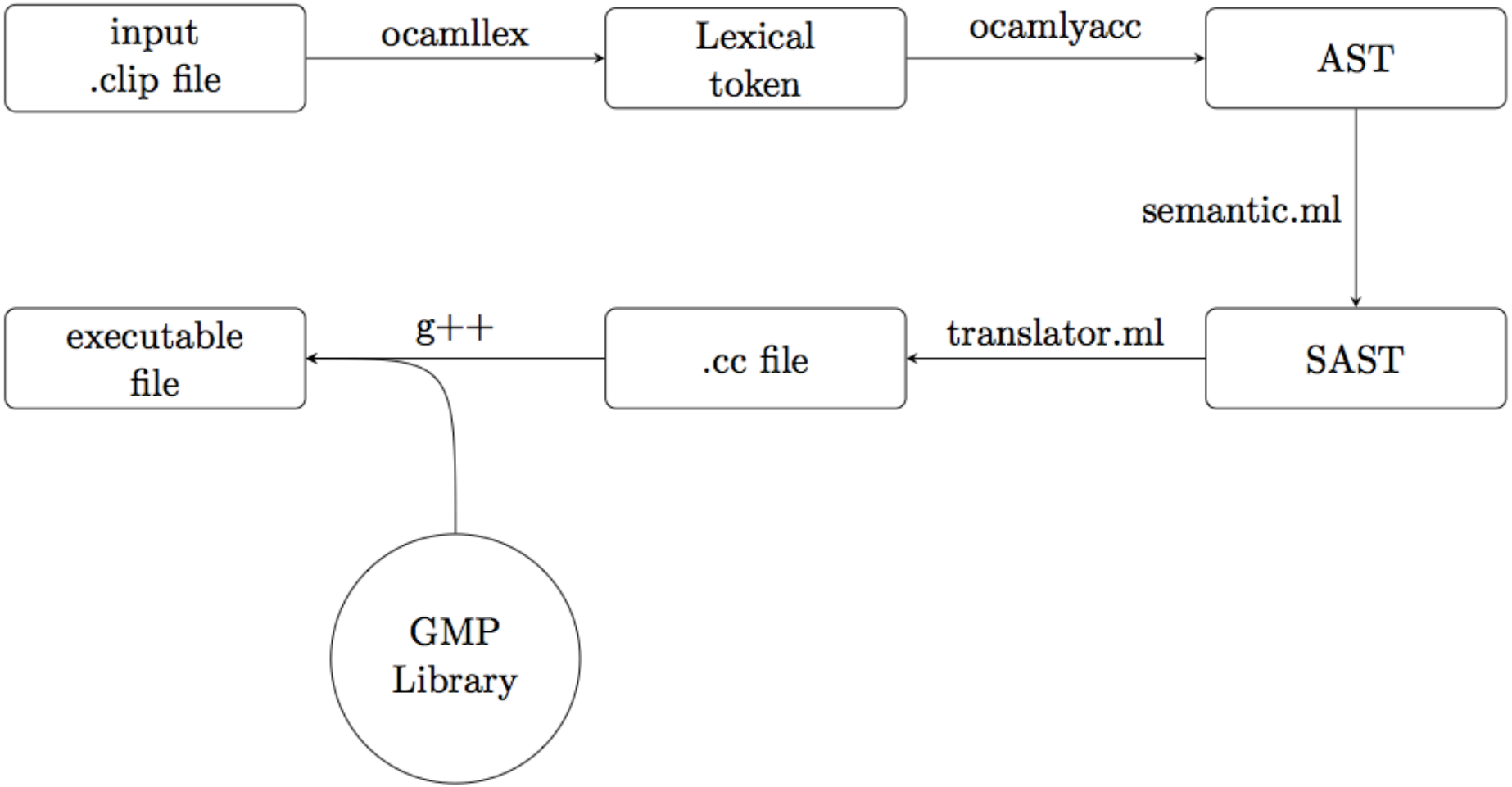
(let <variable:type expression1> expression2)

(map function vector)

(reduce function vector)

(lambda <argument:type> expression)

Architecture



Demo

- 1. GCD
- 2. SHA-3
- 3. RSA

SHA-3

$$(\theta \to \rho \to \pi \to \chi \to \iota) \times 24$$

	64 bits				
	$1010\cdots10$	$0000\cdots11$	$0101\cdots10$	$1110\cdots11$	$0110\cdots00$
	$0101\cdots01$	$1001\cdots01$	$0101\cdots00$	$1111\cdots11$	$0111\cdots11$
	$0000\cdots00$	$1111\cdots11$	$0100\cdots01$	$0100\cdots11$	$0011\cdots11$
	$1000\cdots11$	$0111\cdots01$	$1001\cdots11$	$0000\cdots00$	$1101\cdots10$
$\oplus$	$1111\cdots00$	$0010\cdots10$	$0100\cdots11$	$0000\cdots00$	$1010\cdots10$
	$1000\cdots00$	$0001\cdots10$	$1001\cdots11$	$0101\cdots11$	$0011\cdots00$
$>>> 64$	$0011\cdots00$	$1000\cdots00$	$0001\cdots10$	$1001\cdots11$	$0101\cdots11$
$<<< 63$	$0000\cdots00$	$0100\cdots11$	$1010\cdots11$	$1001\cdots10$	$0100\cdots00$

RSA

$$n = p \cdot q$$

$$N = \phi(n) = (p-1)(q-1)$$

$$e = 65537$$

$$d = e^{-1} \bmod N$$

Public: n, e
Private: N, d

$$m = c^e \bmod n$$

$$c = m^d \bmod n$$