

1 Language

1.1 AST

$$e := x \mid v \mid \text{f_un}(e) \mid \text{f_bin}(e, e) \mid \text{let } x = e \text{ in } e$$

1.2 Typing Rules

$$\frac{x : \tau \in \Gamma}{\Gamma \vdash x : \tau} \text{ (T-VAR)} \quad \frac{}{\vdash v : \text{public}} \text{ (T-VAL)}$$

$$\frac{\Gamma \vdash e : \tau}{\Gamma \vdash \text{f_un}(e) : \tau} \text{ (T-UNFUN)} \quad \frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma \vdash e_2 : \tau_2}{\Gamma \vdash \text{f_bin}(e_1, e_2) : \max(\tau_1, \tau_2)} \text{ (T-BINFUN)}$$

$$\frac{\Gamma \vdash e_1 : \tau_1 \quad \Gamma, x : \tau_1 \vdash e_2 : \tau_2}{\Gamma \vdash \text{let } x = e_1 \text{ in } e_2 : \max(\tau_1, \tau_2)} \text{ (T-LET)}$$

$$\frac{\tau_1 \text{ is secret} \vee \tau_2 \text{ is secret}}{\max(\tau_1, \tau_2) \text{ is secret}} \text{ (T-MAXSECRET)} \quad \frac{\tau_1 \text{ is public} \wedge \tau_2 \text{ is public}}{\max(\tau_1, \tau_2) \text{ is public}} \text{ (T-MAXPUBLIC)}$$