$$\frac{E \vdash M : \mathsf{public} \quad E \vdash M_1 : \mathsf{public} \quad \ldots \quad E \vdash M_k : \mathsf{public} \quad E \vdash P}{E \vdash \mathsf{send}_M\langle M_1, \ldots, M_k\rangle; P}$$

$$\frac{E \vdash M : \mathsf{secret} \quad E \vdash M_1 : \mathsf{secret} \quad E \vdash M_2 : \mathsf{any} \quad E \vdash M_3 : \mathsf{public} \quad E \vdash P}{E \vdash \mathsf{send}_M\langle M_1, M_2, M_3\rangle; P}$$

Only public data may be sent on public channels.

On secret channels, data is always sent in the standard format we have agreed upon.

We consider pairing as left-associative.

For example (M_1, M_2, M_3, M_4) is same as $((M_1, M_2), M_3, M_4)$

Similar rules for inputs.

$$\frac{E \vdash M : \mathsf{public} \quad E, x_1 : \mathsf{public}, \ldots, x_k : \mathsf{public} \vdash P}{E \vdash \mathsf{recv}_M(x_1, \ldots, x_k); P}$$

$$\frac{E \vdash M : \mathsf{secret} \quad E, x_1 : \mathsf{secret}, x_2 : \mathsf{any}, x_3 : \mathsf{public} \vdash P}{E \vdash \mathsf{recv}_M(x_1, x_2, x_3); P}$$

The appropriate class information for the input variables is added to the environment, and the new environment is used for typing the remaining process.

$$\frac{\vdash E}{E \vdash \mathsf{halt}}$$

$$\frac{E \vdash P \qquad E \vdash Q}{E \vdash P \mid Q}$$

$$\frac{E \vdash P}{E \vdash \mathsf{repeat}\ P}$$

$$\frac{E, n : T :: L \vdash P}{E \vdash \mathsf{new}\ n; P}$$

The newly created name can be chosen to be kept secret or can be revealed, and can be chosen to used as a confounder in some message.

$$\boxed{\dfrac{E \vdash M : T \qquad E \vdash N : R \qquad E \vdash P \qquad T, R \in \{\mathsf{public}, \mathsf{secret}\}}{E \vdash \mathsf{check}\ (M == N); P}}$$

Equality checks are not allowed on data of class any to prevent implicit information flow.

Example Consider $P \triangleq \mathsf{recv}_c(y); \mathsf{check}\ (x == y); \mathsf{send}_c\langle 0\rangle; \mathsf{halt}$ where x is the data whose secrecy we are interested in.

Secrecy of x is not maintained. $P[M/x]$ and $P[M'/x]$ are not equivalent for $M \neq M'$.

Consider test $(Q, \overline{d})$ where $Q \triangleq \mathsf{send}_c\langle M\rangle; \mathsf{recv}_c(z); \mathsf{send}_d\langle 0\rangle; \mathsf{halt}$.

$P[M/x] \mid Q$ passes the test:

$P[M/x] \mid Q \xrightarrow{\tau} \mathsf{check}\ (M = M); \mathsf{send}_c\langle 0\rangle; \mathsf{halt} \mid \mathsf{recv}_c(z); \mathsf{send}_d\langle 0\rangle; \mathsf{halt} \xrightarrow{\tau}$
$\mathsf{halt} \mid \mathsf{send}_d\langle 0\rangle; \mathsf{halt} \xrightarrow{\overline{d}} \langle 0\rangle(\mathsf{halt} \mid \mathsf{halt})$

$P[M'/x] \mid Q$ does not pass the test.

Similarly, case analysis on data of class any are disallowed.

$$\frac{E \vdash M : T \qquad E, x : T, y : T \vdash P \qquad T \in \{\mathsf{public}, \mathsf{secret}\}}{E \vdash \mathsf{let}\ (x, y) = M; P}$$

$$\frac{E \vdash M : T \qquad E \vdash P \qquad E, x : T \vdash Q \qquad T \in \{\mathsf{secret}, \mathsf{public}\}}{E \vdash \mathsf{case}\ M\ \mathsf{of}\ 0 : P,\ \mathsf{succ}\ (x) : Q}$$

Decryption

$$\frac{E \vdash L : T \quad E \vdash N : \mathsf{public} \quad E, x_1 : T, \ldots, x_k : T \vdash P \quad T \in \{\mathsf{secret}, \mathsf{public}\}}{E \vdash \mathsf{case}\ L\ \mathsf{of}\ \{x_1, \ldots, x_k\}_N : P}$$

$$\frac{\begin{array}{c} E \vdash L : T \qquad E \vdash N : \mathsf{secret} \qquad T \in \{\mathsf{secret}, \mathsf{public}\} \\ E, x_1 : \mathsf{secret}, x_2 : \mathsf{any}, x_3 : \mathsf{public}, x_4 : \mathsf{any} \vdash P \end{array}}{E \vdash \mathsf{case}\ L\ \mathsf{of}\ \{x_1, x_2, x_3, x_4\}_N : P}$$

The confounder x_4 in the second rule is assumed to be of type any because we have no more information about it.

Typing implies noleak of information

Suppose

- $\vdash E$
- all variables in $dom(E)$ are of level any and all names in $dom(E)$ are of level public.
- $E \vdash P$
- P has free variables $x_1, \ldots, x_k$
- $fn(M_i), fn(M_i') \subseteq dom(E)$ for $1 \leq i \leq k$.

then $P[M_1/x_1, \ldots, M_k/x_k] \simeq P[M_1/x_1, \ldots, M_k/x_k]$

Well typed processes maintain secrecy of the free variables $(x_1, \ldots, x_k)$, i.e. they are not leaked.

Our previous example $P \triangleq \mathsf{recv}_c(y); \mathsf{check}\ (x == y); \mathsf{send}_c\langle 0\rangle; \mathsf{halt}$

We take $E \triangleq \{x : \mathsf{any}, c : \mathsf{public} :: \{n\}_0\}$. c is not meant to be used as a confounder, hence we have the dummy term $\{n\}_0$.

We have $\vdash E$.

In order to show $E \vdash P$ we need to find some T such that

$E, y : \mathsf{public} \vdash \mathsf{check}\ (x == y); \mathsf{send}_c\langle 0\rangle; \mathsf{halt}$.

But this is impossible because equality checks should not involve data of class any.

Hence the process doesn't type-check, as required.

Consider $P \triangleq \mathsf{new}\ K; \mathsf{new}\ m; \mathsf{new}\ n; \mathsf{send}_c\langle\{m, x, 0, n\}_K\rangle; \mathsf{halt}$.

We take $E \triangleq \{x : \mathsf{any}, c : \mathsf{public} :: \{n\}_0\}$. We have $\vdash E$.

To show $E \vdash P$ we choose
$E' \triangleq E, K : \mathsf{secret} :: \{K\}_0, m : \mathsf{secret} :: \{m\}_0, n : \mathsf{secret} :: \{m, x, 0, n\}_K$
and show that $E' \vdash \mathsf{send}_c\langle\{m, x, 0, n\}_K\rangle; \mathsf{halt}$.

This is ok because $E' \vdash m : \mathsf{secret}$, $E' \vdash x : \mathsf{any}$, $E' \vdash 0 : \mathsf{public}$, $E' \vdash n : \mathsf{secret}$, $E' \vdash K : \mathsf{secret}$ and $E' \vdash \mathsf{halt}$.