4. Eq. theories & Static Equiv

$u \oplus u = 0 \qquad u \oplus 0 = u$

$T(\mathcal{F}, \mathcal{X}, \mathcal{N})$

$E = \{ \ldots, u = v, \ldots \}$

$=_E \qquad u = v \in E \Rightarrow u\theta = v\theta$

$u_1 =_E v_1 \quad \cdots \quad u_n =_E v_n$

$\Rightarrow f(u_1 \cdots u_n) =_E f(v_1 \cdots v_n)$

$E_\oplus$ $x \oplus (y \oplus z) = (x \oplus y) \oplus z$. $x \oplus x = 0$

$x \oplus y = y \oplus x$. $x \oplus 0 = x$

Ex. $u = k_1 \oplus k_2$ $v = k_2 \oplus k_3$ $w = k_1 \oplus k_3$

$u \oplus v = (k_1 \oplus k_2) \oplus (k_2 \oplus k_3) =_C k_1 \oplus (k_2 \oplus (k_2 \oplus k_3))$

$=_E k_1 \oplus ((k_2 \oplus k_2) \oplus k_3)$

$=_E k_1 \oplus (0 \oplus k_3)$

$=_E k_1 \oplus (k_3 \oplus 0)$

$=_E k_1 \oplus k_3 = w$

$$exp(exp(x,y),z) = exp(exp(x,z),y)$$

$$(g^x)^y = (g^y)^x$$

Diffie Hellmann

$A \to B : g^x$

$B \to A : g^y$

$A : x \cdot g^y \cdot (g^y)^x$

$B : y \cdot g^x \cdot (g^x)^y$

u_{E_y}

$$F_{Std} = \{ senc, aenc \ \ldots \}$$

$$F_{dec} = \{ sdec, adec, fst, snd \}$$

$$E_{Dy}: \begin{cases} sdec(senc(x,y),y) = x \\ adec(aenc(x,pk(y)),y) = x \\ fst(\langle x,y \rangle) = x \\ snd(\langle x,y \rangle) = y \end{cases}$$

Deduction

$$\frac{t_1 \quad \dots \quad t_n}{f(t_1, \dots, t_n)} \qquad \frac{t}{t'} \text{ if } t =_E t'$$

Ex:

$E_\oplus \cup E_{DJ}$ $\quad S = \{\{a\}_{a\oplus c}, a\oplus b, b\oplus c\}$

$S \vdash_{E_\oplus \cup E_{DJ}} a$

$$\dfrac{\dfrac{\{a\}_{a\oplus c} \qquad \dfrac{a\oplus b \qquad b\oplus c}{(a\oplus b)\oplus(b\oplus c)} =_C}{a\oplus c}}{\dfrac{\{\{a\}_{a\oplus c}\}^{-1}_{a\oplus c} \qquad a\oplus c}{a} =_E}$$

Prop 4.1. If $S \vdash_\varepsilon t$ then $\exists C.\ n(C) = \phi$

$\exists t_1, \ldots, t_n \in S.\ t = C[t_1, \ldots, t_n]$

and vice versa

$S = \{\alpha\{_{\alpha \oplus c}, \alpha \oplus b, b \oplus c\}$

$S \vdash_\varepsilon \alpha \Rightarrow \exists C.\ C[\lambda\alpha\{_{\alpha \oplus c}, \alpha \oplus b, b \oplus c]] = \alpha$

$C[x, y, z] = \{x\}^{-1}_{(y \oplus z)} =_\varepsilon \alpha$

Equivelence of Frames

Def (Frame) $\varphi = \nu \tilde{n}\, \theta = \nu \tilde{n} \{ t_1/x_1 \cdots t_m/x_m \{$

$Dom(\varphi) = Dom(\theta)$

Ex: $\varphi = \nu k \{ 1/x_0, 0/x_1, \{0\{k/x_2 \{$

Def (Deduction) $T(F, \mathcal{X}, \mathcal{N})$

$\varphi\, t_E\, t$ if $Dom(\varphi) \cup (\mathcal{N} \setminus \tilde{n})\, t_E\, t$

Ex: $\varphi_1 = \nu n, k\ \theta_1, \theta_1 = \{\{\langle n,n\rangle\}_{k/x}, {}^{k}/_{y}\}$

$\varphi_1 \overset{?}{\vdash_E} n \Leftrightarrow \{\langle n,n\rangle\}_k, k, a, b, c \ldots \overset{?}{\vdash_E} n$

$C[x,y] = fst(\{x\}_y^{-1})$

$$\frac{\{\langle n,n\rangle\}_k \qquad k}{\{\{\langle n,n\rangle\}_k\}_k^{-1}}$$

$$\frac{\langle n,n\rangle}{n}$$

$\varphi_0 = \{0/x, 1/y\}$ $\varphi_1 = \{1/x, 0/y\}$

Def $\varphi_1 =_\alpha \varphi_2$

$(\Pi =_E N)\varphi$ iff . $\exists \tilde{n}, \theta$. st. $\varphi =_\alpha \underline{\underline{v \tilde{n} \theta}}$

, Π, N are free w.r.t. $v \tilde{n} \theta$

. $\Pi\theta =_E N\theta$

Def (Static equivalence)

$\varphi_1 \sim_E \varphi_2$ iff $Dom(\varphi_1) = Dom(\varphi_2)$

$\forall \Pi, N.\ (\Pi =_E N)\varphi_1$ iff $(\Pi =_E N)\varphi_2$

Ex: $\varphi_1 = \{0/x, 1/y\}$ $\varphi_2 = \{1/x, 0/y\}$

$\varphi_1 \not\perp_E \varphi_2$ $\quad \Pi = x$

$N = 0$

$(x = 0)\varphi_2$ while $(x \neq 0)\varphi_2$

Ex: $\varphi_1 = DK\{aenc(0, pk(k)/x, pk(k)/y\}$

$\varphi_2 = DK\{aenc(1, pk(k)/x, pk(k)/y\}$

$\varphi_1 \overset{?}{\sim} \varphi_2$ $\quad M = x \quad N = aenc(0, y)$.

$(x = N)\varphi_1$ $\quad (x \neq N)\varphi_2$

Ex: $\varphi_1 = \nu k, n \{ \mathrm{senc}(\langle 0, n \rangle, pk(k))/_{\mathrm{senc}}, pk(k)/_{g} \}$

$\varphi_2 = \nu k, n \{ \mathrm{senc}(\langle 1, n \rangle, pk(k))/_{\mathrm{senc}}, pk(k)/_{g} \}$

$\mathrm{senc}(\langle 0, n \rangle, y)$

$\varphi_1 \sim \varphi_2$

Proverif Example

```
channel c.
fun aenc(bitstring, bitstring):
bitstring.
fun pk(bitstring): bitstring.
reduc forall x:bitstring, y:bitstring;
adec(aenc(x,pk(y)),y) = x.

const zero: bitstring.
const one: bitstring.

process new n: bitstring; new k:
bitstring; out(c, aenc(diff[zero,one],
pk(k))); out(c, pk(k))
```