BAN inference rules

Message meaning rules for shared keys:

$$MM - SK \ \ \frac{P \mid\equiv (Q \leftrightarrow^{K} P), P \triangleleft \{X\}_K}{P \mid\equiv (Q \mid\sim X)} \qquad \frac{P \textbf{ believes } (Q \leftrightarrow^{K} P), P \textbf{ sees } \{X\}_K}{P \textbf{ believes } (Q \textbf{ said } X)}$$

Message meaning rules for public keys:

$$MM - PK \ \ \frac{P \mid\equiv \mapsto^{K} Q, P \triangleleft \{X\}_{K^{-1}}}{P \mid\equiv (Q \mid\sim X)}$$

The nonce-verification rule:

$$NV \ \ \frac{P \mid\equiv \sharp(X), P \mid\equiv Q \mid\sim X}{P \mid\equiv (Q \mid\equiv X)} \qquad NV \ \ \frac{P \textbf{ believes fresh}(X), P \textbf{ believes } Q \textbf{ said } X}{P \textbf{ believes } (Q \textbf{ believes } X)}$$

The jurisdiction rule:

$$JR \ \ \frac{P \mid\equiv Q \mid\Rightarrow X, P \mid\equiv Q \mid\equiv X}{P \mid\equiv X} \qquad JR \ \ \frac{P \textbf{ believes } (Q \textbf{ controls } X), P \textbf{ believes } (Q \textbf{ believes } X}{P \textbf{ believes } X}$$

Belief and components:

$$BC1 \ \ \frac{P \mid\equiv X, P \mid\equiv Y}{P \mid\equiv (X, Y)} \qquad BC2 \ \ \frac{P \mid\equiv (X, Y)}{P \mid\equiv X}$$

$$BC3 \ \ \frac{P \mid\equiv Q \mid\equiv (X, Y)}{P \mid\equiv Q \mid\equiv X} \qquad BC4 \ \ \frac{P \mid\equiv Q \mid\sim (X, Y)}{P \mid\equiv Q \mid\sim X}$$

Seeing and components:

$$SC1 \ \ \frac{P \triangleleft (X, Y)}{P \triangleleft X} \qquad SC2 \ \ \frac{P \triangleleft \langle X \rangle_Y}{P \triangleleft X}$$

$$SC3 \ \ \frac{P \mid\equiv Q \leftrightarrow^{K} P, P \triangleleft \{X\}_K}{P \triangleleft X} \qquad SC4 \ \ \frac{P \mid\equiv \mapsto^{K} P, P \triangleleft \{X\}_K}{P \triangleleft X}$$

$$SC5 \ \ \frac{P \mid\equiv \mapsto^{K} Q, P \triangleleft \{X\}_{K^{-1}}}{P \triangleleft X}$$

Nonces concatenation

$$NC \ \ \frac{P \mid\equiv \sharp(X)}{P \mid\equiv \sharp(X, Y)}$$

Commutativity of secrets:

$$\frac{P \mid\equiv R \rightleftharpoons^{X} R'}{P \mid\equiv R' \rightleftharpoons^{X} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \rightleftharpoons^{X} R'}{P \mid\equiv Q \mid\equiv R' \rightleftharpoons^{X} R}$$

Commutativity of keys:

$$\frac{P \mid\equiv R \leftrightarrow^{X} R'}{P \mid\equiv R' \leftrightarrow^{X} R} \qquad \frac{P \mid\equiv Q \mid\equiv R \leftrightarrow^{X} R'}{P \mid\equiv Q \mid\equiv R' \leftrightarrow^{X} R}$$