Beispiel zur Übersetzung von PSP in MP–Code

in/out X;

var E;

proc F;

if $1 < X$ **then begin**

$E := E * X$;

$X := X - 1$;

$F()$

end;

B_F $\|$ Γ_F } $\tilde{\Delta}$ } Δ

begin

$E := 1$;

$F()$;

$X := E$

end. } Γ

$$\textbf{trans}(\textbf{in/out}\ X;\Delta\Gamma) \quad = \quad 1 : \mathrm{CALL}(a_\Gamma, 0, 1);$$
$$2 : \mathrm{JMP}(0);$$
$$\textbf{bt}(\Delta\Gamma, st_{I/O}, a_\Gamma, 1)$$

mit $st_{I/O}(X) = (\textbf{var}, 0, 1)$

$$
\begin{aligned}
\mathbf{bt}(\Delta\Gamma, st_{I/O}, a_\Gamma, 1) &= \mathbf{dt}(\Delta, \mathbf{up}(\Delta, st_{I/O}, a_1, 1), a_1, 1) \\
&\quad \mathbf{ct}(\Gamma, \mathbf{up}(\Delta, st_{I/O}, a_1, 1), a_\Gamma, 1) \\
&\quad a_2 : \mathrm{RET};
\end{aligned}
$$

$$
\mathbf{up}(\Delta, st_{I/O}, a_1, 1) = \underbrace{st_{I/O}[E/(\mathbf{var}, 1, 1), F/(\mathbf{proc}, a_{11}, 1, 0)]}_{\overline{st}}
$$

$$
\begin{aligned}
\mathbf{dt}(\Delta, \overline{st}, a_1, 1) &= \mathbf{bt}(B_F, \overline{st}, a_{11}, 2) \\
&= \mathbf{ct}(\Gamma_F, \overline{st}, a_{11}2, 2) \\
&\quad a_3 : \mathrm{RET};
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{ct}(\Gamma, \overline{st}, a_\Gamma, 1) &= a_\Gamma : \mathrm{LIT}(1); \\
&\quad \mathrm{STO}(0,1); \\
&\quad \mathrm{CALL}(a_{11}, 0, 0); \\
&\quad \mathrm{LOAD}(0,1); \\
&\quad \mathrm{STO}(1,1);
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{ct}(\Gamma_F, \overline{st}, a_{11}, 2) &= \mathbf{et}(1 < x, \overline{st}, a_{11}, 2) \\
&\quad a_4 : \mathrm{JFALSE}(a_5); \\
&\quad \mathbf{ct}(\mathbf{begin} \ldots \mathbf{end}, \overline{st}, a_4 + 1, 2) \\
&\quad a_5 :
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{et}(1 < x, \overline{st}, a_{11}, 2) &= a_{11} : \mathrm{LIT}(1); \\
&\quad \mathrm{LOAD}(2,1); \\
&\quad \mathrm{LT};
\end{aligned}
$$

$$
\begin{aligned}
\mathbf{ct}(\mathbf{begin} \ldots \mathbf{end}, \overline{st}, a_4 + 1, 2) &= \mathbf{ct}(E := E * X, \overline{st}, a_4 + 1, 2) \\
&\quad \mathbf{ct}(X := X - 1, \overline{st}, a_6, 2) \\
&\quad \mathbf{ct}(F(), \overline{st}, a_7, 2) \\
&= a_4 + 1 : \mathrm{LOAD}(1,1); \\
&\quad \mathrm{LOAD}(2,1); \\
&\quad \mathrm{MULT}; \\
&\quad \mathrm{STO}(1,1); \\
&\quad \mathrm{LOAD}(2,1); \\
&\quad \mathrm{LIT}(1); \\
&\quad \mathrm{SUB}; \\
&\quad \mathrm{STO}(2,1); \\
&\quad \mathrm{CALL}(a_{11}, 1, 0)
\end{aligned}
$$

Ergebnis der Übersetzung:

$\mathbf{trans}(\mathbf{in}/\mathbf{out}\ X;\Delta\Gamma) =$

$1:$	$\mathrm{CALL}(a_\Gamma,0,1);$	Also:
$2:$	$\mathrm{JMP}(0);$	
$a_{11}:$	$\mathrm{LIT}(1);$	$a_{11}=3$
	$\mathrm{LOAD}(2,1);$	
	$\mathrm{LT};$	
$a_4:$	$\mathrm{JFALSE}(a_5);$	$a_4=6$
	$\mathrm{LOAD}(1,1);$	
	$\mathrm{LOAD}(2,1);$	
	$\mathrm{MULT};$	
	$\mathrm{STO}(1,1);$	
	$\mathrm{LOAD}(2,1);$	
	$\mathrm{LIT}(1);$	
	$\mathrm{SUB};$	
	$\mathrm{STO}(2,1);$	
	$\mathrm{CALL}(a_{11},1,0);$	
$a_3:a_5:$	$\mathrm{RET};$	$a_3=16=a_5$
$a_\Gamma:$	$\mathrm{LIT}(1);$	$a_\Gamma=17$
	$\mathrm{STO}(0,1);$	
	$\mathrm{CALL}(a_{11},0,0);$	
	$\mathrm{LOAD}(0,1);$	
	$\mathrm{STO}(1,1);$	
$a_2:$	$\mathrm{RET};$	$a_2=22$

Berechnungsprotokoll für $X = 3$:

$m \in BZ$	$d \in DK$	$p \in PK$
1	ε	0 : 0 : 0 : 3
17	ε	4 : 3 : 2 : 0 : 0 : 0 : 0 : 3
18	1	4 : 3 : 2 : 0 : 0 : 0 : 0 : 3
19	ε	4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
3	ε	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
4	1	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
5	1 : 3	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
6	1	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
7	ε	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
8	1	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
9	1 : 3	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
10	3	3 : 2 : 20 : 4 : 3 : 2 : 1 : 0 : 0 : 0 : 3
11	ε	3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 3
12	3	3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 3
13	3 : 1	3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 3
14	2	3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 3
15	ε	3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
3	ε	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
4	1	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
5	1 : 2	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
6	1	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
7	ε	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
8	3	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
9	3 : 2	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
10	6	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 3 : 0 : 0 : 0 : 2
11	ε	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 2
12	2	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 2
13	2 : 1	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 2
14	1	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 2
15	ε	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
3	ε	9 : 2 : 16 : 6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
4	1	9 : 2 : 16 : 6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
5	1 : 1	9 : 2 : 16 : 6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
6	0	9 : 2 : 16 : 6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
16	ε	9 : 2 : 16 : 6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
16	ε	6 : 2 : 16 : 3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
16	ε	3 : 2 : 20 : 4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
20	ε	4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
21	6	4 : 3 : 2 : 6 : 0 : 0 : 0 : 1
22	ε	4 : 3 : 2 : 6 : 0 : 0 : 0 : 6
0	ε	0 : 0 : 0 : 6