Model: DES (Data Encryption Standard)
Type: P/T Net
Origin: Industrial (NIST (USA))

since
MCC 2016

Wendelin Serwe and Hubert Garavel
wendelin.serwe@inria.fr

This form is a summary description of the model entitled "DES (Data Encryption Standard)" proposed for the Model Checking Contest @ Petri Nets. Models can be given in several instances parameterized by scaling parameters. Colored nets can be accompanied by one or many equivalent, unfolded P/T nets. Models are given together with property files (possibly, one per model instance) giving a set of properties to be checked on the model.

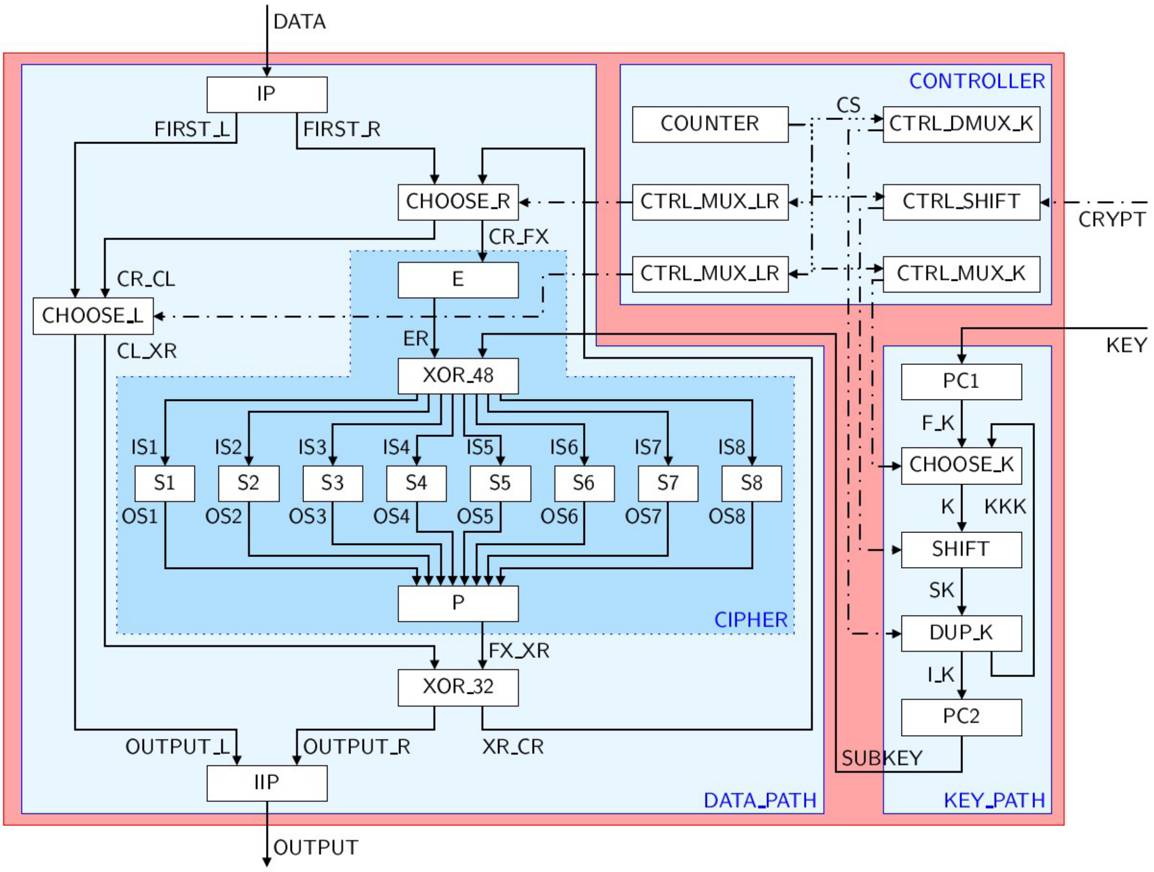
Description

The Data Encryption Standard (DES) is a symmetric-key encryption algorithm, which has been for almost thirty years a Federal Information Processing Standard. The DES is specified by a data-flow diagram, i.e., a set of blocks communicating by message passing. Such an architecture is naturally asynchronous (there is no need for a global clock synchronizing the various blocks) and naturally lends itself to analysis with process calculi.

This collection of P/T nets was derived from an LNT model of the DES. Each instance was first translated to LOTOS, and then to an interpreted Petri net using the CADP toolbox. Finally, a P/T net was obtained by stripping out all data-related information (variables, types, assignments, guards, etc.) from the interpreted Petri net, leading to a NUPN (Nested-Unit Petri Net) model translated to PNML using the CÆSAR.BDD tool.

Each instance of the model is parameterized by the number N of encryption operations to be executed in sequence, i.e., the length of the finite sequence of data given as input to the DES algorithm. The particular case $N = 0$ corresponds to an infinite (i.e., cyclic) sequence of inputs.

Each instance is also parameterized by its version V, which specifies how the NUPN has been produced from the LOTOS specification. V is either equal to "*a*" if the NUPN has been generated *after* applying all the structural and data-flow optimizations of the CÆSAR compiler for LOTOS, or to "*b*" if the NUPN has been generated *before* these optimizations.



Dataflow architecture of the DES

References

[1] National Institute of Standards and Technology. *Data Encryption Standard (DES)*. Federal Information Processing Standards Publication 46-3, 1999. Available from http://csrc.nist.gov/publications/fips/fips46-3/fips46-3.pdf.

[2] Wendelin Serwe. *Formal Specification and Verification of Fully Asynchronous Implementations of the Data Encryption Standard*. In Rob van Glabbeek, Jan Friso Groote, and Peter Höfner, Proceedings of the first Workshop on Models for Formal Analysis of Real Systems (MARS 2015), November 2015, Suva, Fiji. Electronic Proceedings in Theoretical Computer Science, Volume 196, pages 61-147, November 2015. Available from http://dx.doi.org/10.4204/EPTCS.196.6 and https://hal.inria.fr/hal-01227999/en

[3] http://cadp.inria.fr/demos.html – look for demo_38

Scaling parameter

Parameter name	**Parameter description**	**Chosen parameter values**
(N, V)	N is the input sequence length and V is the version defined above	$\{0,1,2,5,10,20,30,40,50,60\} \times \{a,b\}$

Size of the model

Parameter	**Number of places**	**Number of transitions**	**Number of arcs**	**Number of units**	**HWB code**
$N = 0, V = a$	115	76	373	56	3–53–109
$N = 0, V = b$	271	230	658	99	17–53–166
$N = 1, V = a$	119	76	381	60	3–57–113
$N = 1, V = b$	284	235	683	107	18–57–178
$N = 2, V = a$	123	80	400	60	3–57–117
$N = 2, V = b$	288	239	699	107	18–57–178
$N = 5, V = a$	135	92	457	60	3–57–121
$N = 5, V = b$	300	251	747	107	18–57–182
$N = 10, V = a$	155	112	552	60	3–57–125
$N = 10, V = b$	320	271	827	107	18–57–186
$N = 20, V = a$	195	152	742	60	3–57–129
$N = 20, V = b$	360	311	987	107	18–57–190
$N = 30, V = a$	234	191	926	60	3–57–129
$N = 30, V = b$	399	350	1143	107	18–57–190
$N = 40, V = a$	274	231	1116	60	3–57–133
$N = 40, V = b$	439	390	1303	107	18–57–194
$N = 50, V = a$	314	271	1306	60	3–57–133
$N = 50, V = b$	479	430	1463	107	18–57–194
$N = 60, V = a$	354	311	1496	60	3–57–133
$N = 60, V = b$	519	470	1623	107	18–57–194

Structural properties

ordinary — *all arcs have multiplicity one* .... yes
simple free choice — *all transitions sharing a common input place have no other input place* .... no [(a)]
extended free choice — *all transitions sharing a common input place have the same input places* .... no [(b)]
state machine — *every transition has exactly one input place and exactly one output place* .... no [(c)]
marked graph — *every place has exactly one input transition and exactly one output transition* .... no [(d)]
connected — *there is an undirected path between every two nodes (places or transitions)* .... yes [(e)]

[(a)] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[(b)] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[(c)] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[(d)] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).
[(e)] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).

strongly connected — *there is a directed path between every two nodes (places or transitions)* . . . . no [f]

source place(s) — *one or more places have no input transitions* . . . . yes [g]

sink place(s) — *one or more places have no output transitions* . . . . ? [h]

source transition(s) — *one or more transitions have no input places* . . . . no [i]

sink transitions(s) — *one or more transitions have no output places* . . . . ? [j]

loop-free — *no transition has an input place that is also an output place* . . . . ? [k]

conservative — *for each transition, the number of input arcs equals the number of output arcs* . . . . no [l]

subconservative — *for each transition, the number of input arcs equals or exceeds the number of output arcs* . . . . . . no [m]

nested units — *places are structured into hierarchically nested sequential units* [n] . . . . yes

Behavioural properties

safe — *in every reachable marking, there is no more than one token on a place* . . . . yes [o]

dead place(s) — *one or more places have no token in any reachable marking* . . . . ? [p]

dead transition(s) — *one or more transitions cannot fire from any reachable marking* . . . . ? [q]

deadlock — *there exists a reachable marking from which no transition can be fired* . . . . ? [r]

reversible — *from every reachable marking, there is a transition path going back to the initial marking* . . . . ? [s]

live — *for every transition t, from every reachable marking, one can reach a marking in which t can fire* . . . . ? [t]

[f] from place 1 one cannot reach place 0.

[g] place 0 is a source place.

[h] stated by CÆSAR.BDD version 2.6 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).

[i] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).

[j] stated by CÆSAR.BDD version 2.6 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).

[k] stated by CÆSAR.BDD version 2.6 to be true on 10 instance(s) out of 20, and false on the remaining 10 instance(s).

[l] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).

[m] stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of N × 2 values of V).

[n] the definition of Nested-Unit Petri Nets (NUPN) is available from `http://mcc.lip6.fr/nupn.php`

[o] safe by construction – stated by the CÆSAR compiler.

[p] stated by CÆSAR.BDD version 3.3 to be false on 4 instance(s) out of 20, and unknown on the remaining 16 instance(s).

[q] stated by CÆSAR.BDD version 2.6 to be false on 4 instance(s) out of 20, and unknown on the remaining 16 instance(s).

[r] stated by CÆSAR.BDD version 2.6 to be true on 4 instance(s) out of 20, and unknown on the remaining 16 instance(s).

[s] stated by CÆSAR.BDD version 2.6 to be false on 4 instance(s) out of 20, and unknown on the remaining 16 instance(s).

[t] stated by CÆSAR.BDD version 2.6 to be false on 4 instance(s) out of 20, and unknown on the remaining 16 instance(s).

Size of the marking graphs

Parameter	Number of reachable markings	Number of transition firings	Max. number of tokens per place	Max. number of tokens per marking
$N = 0, V = a$	2.4197e+10 [u]	?	1	$\in [41, 53]$ [v]
$N = 0, V = b$	$\geq$ 5.35317e+15 [w]	?	1 [x]	$\in [41, 53]$ [y]
$N = 1, V = a$	1.0858e+08 [z]	?	1	$\in [43, 57]$ [aa]
$N = 1, V = b$	$\geq$ 6.78133e+15 [ab]	?	1 [ac]	$\in [45, 57]$ [ad]
$N = 2, V = a$	4.95322e+09 [ae]	?	1	$\in [44, 57]$ [af]
$N = 2, V = b$	$\geq$ 5.25147e+15 [ag]	?	1 [ah]	$\in [45, 57]$ [ai]
$N = 5, V = a$	2.30998e+11 [aj]	?	1 [ak]	$\in [43, 57]$ [al]
$N = 5, V = b$	$\geq$ 5.77614e+15 [am]	?	1 [an]	$\in [45, 57]$ [ao]
$N = 10, V = a$	$\geq$ 2.65612e+11 [ap]	?	1 [aq]	$\in [45, 57]$ [ar]
$N = 10, V = b$	$\geq$ 5.77614e+15 [as]	?	1 [at]	$\in [45, 57]$ [au]
$N = 20, V = a$	$\geq$ 9.25792e+11 [av]	?	1 [aw]	$\in [45, 57]$ [ax]
$N = 20, V = b$	$\geq$ 5.77614e+15 [ay]	?	1 [az]	$\in [45, 57]$ [ba]
$N = 30, V = a$	$\geq$ 4.18122e+11 [bb]	?	1 [bc]	$\in [45, 57]$ [bd]
$N = 30, V = b$	$\geq$ 5.77614e+15 [be]	?	1 [bf]	$\in [45, 57]$ [bg]
$N = 40, V = a$	$\geq$ 2.65919e+11 [bh]	?	1 [bi]	$\in [45, 57]$ [bj]
$N = 40, V = b$	$\geq$ 5.77614e+15 [bk]	?	1 [bl]	$\in [45, 57]$ [bm]
$N = 50, V = a$	$\geq$ 4.70293e+11 [bn]	?	1 [bo]	$\in [45, 57]$ [bp]
$N = 50, V = b$	$\geq$ 5.77614e+15 [bq]	?	1 [br]	$\in [45, 57]$ [bs]
$N = 60, V = a$	$\geq$ 2.65919e+11 [bt]	?	1 [bu]	$\in [45, 57]$ [bv]
$N = 60, V = b$	$\geq$ 5.77614e+15 [bw]	?	1 [bx]	$\in [45, 57]$ [by]

[u] stated by CÆSAR.BDD version 2.6.
[v] upper bound given by the number of leaf units.
[w] stated by CÆSAR.BDD version 3.3.
[x] stated by the CÆSAR compiler.
[y] upper bound given by the number of leaf units.
[z] stated by CÆSAR.BDD version 2.6.
[aa] upper bound given by the number of leaf units.
[ab] stated by CÆSAR.BDD version 3.3.
[ac] stated by the CÆSAR compiler.
[ad] upper bound given by the number of leaf units.
[ae] stated by CÆSAR.BDD version 2.6.
[af] upper bound given by the number of leaf units.
[ag] stated by CÆSAR.BDD version 3.3.
[ah] stated by the CÆSAR compiler.
[ai] upper bound given by the number of leaf units.
[aj] stated by CÆSAR.BDD version 2.6.
[ak] stated by the CÆSAR compiler.
[al] upper bound given by the number of leaf units.
[am] stated by CÆSAR.BDD version 3.3.
[an] stated by the CÆSAR compiler.
[ao] upper bound given by the number of leaf units.
[ap] stated by CÆSAR.BDD version 2.6.
[aq] stated by the CÆSAR compiler.
[ar] upper bound given by the number of leaf units.
[as] stated by CÆSAR.BDD version 3.3.
[at] stated by the CÆSAR compiler.
[au] upper bound given by the number of leaf units.
[av] stated by CÆSAR.BDD version 2.6.
[aw] stated by the CÆSAR compiler.
[ax] upper bound given by the number of leaf units.
[ay] stated by CÆSAR.BDD version 3.3.
[az] stated by the CÆSAR compiler.
[ba] upper bound given by the number of leaf units.
[bb] stated by CÆSAR.BDD version 2.6.
[bc] stated by the CÆSAR compiler.
[bd] upper bound given by the number of leaf units.
[be] stated by CÆSAR.BDD version 3.3.

[bf] stated by the CÆSAR compiler.

[bg] upper bound given by the number of leaf units.

[bh] stated by CÆSAR.BDD version 2.6.

[bi] stated by the CÆSAR compiler.

[bj] upper bound given by the number of leaf units.

[bk] stated by CÆSAR.BDD version 3.3.

[bl] stated by the CÆSAR compiler.

[bm] upper bound given by the number of leaf units.

[bn] stated by CÆSAR.BDD version 2.6.

[bo] stated by the CÆSAR compiler.

[bp] upper bound given by the number of leaf units.

[bq] stated by CÆSAR.BDD version 3.3.

[br] stated by the CÆSAR compiler.

[bs] upper bound given by the number of leaf units.

[bt] stated by CÆSAR.BDD version 2.6.

[bu] stated by the CÆSAR compiler.

[bv] upper bound given by the number of leaf units.

[bw] stated by CÆSAR.BDD version 3.3.

[bx] stated by the CÆSAR compiler.

[by] upper bound given by the number of leaf units.