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


Scaling parameter

<table>
<thead>
<tr>
<th>Parameter name</th>
<th>Parameter description</th>
<th>Chosen parameter values</th>
</tr>
</thead>
<tbody>
<tr>
<td>((N, V))</td>
<td>(N) is the input sequence length and (V) is the version defined above</td>
<td>({0, 1, 2, 5, 10, 20, 30, 40, 50, 60} \times {a, b})</td>
</tr>
</tbody>
</table>

Size of the model

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

Structural properties

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

\(^{(a)}\) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of \(N \times 2\) values of \(V\)).
\(^{(b)}\) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of \(N \times 2\) values of \(V\)).
\(^{(c)}\) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of \(N \times 2\) values of \(V\)).
\(^{(d)}\) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of \(N \times 2\) values of \(V\)).
\(^{(e)}\) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of \(N \times 2\) values of \(V\)).
strongly connected — there is a directed path between every two nodes (places or transitions)  

source place(s) — one or more places have no input transitions  
sink place(s) — one or more places have no output transitions  

source transition(s) — one or more transitions have no input places  
sink transitions(s) — one or more transitions have no output places  

loop-free — no transition has an input place that is also an output place  

conservative — for each transition, the number of input arcs equals the number of output arcs  

subconservative — for each transition, the number of input arcs equals or exceeds the number of output arcs  

nested units — places are structured into hierarchically nested sequential units  

Behavioural properties

safe — in every reachable marking, there is no more than one token on a place  

deadlock — there exists a reachable marking from which no transition can be fired  

reversible — from every reachable marking, there is a transition path going back to the initial marking  

quasi-live — for every transition $t$, there exists a reachable marking in which $t$ can fire  

live — for every transition $t$, from every reachable marking, one can reach a marking in which $t$ can fire  


(f) from place 1 one cannot reach place 0.  

(s) place 0 is a source place.  

(b) 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 $N \times 2$ values of $V$).  

(l) stated by CÆSAR.BDD version 2.6 on 10 instances (10 values of $N \times 2$ values of $V$).  

(k) stated by CÆSAR.BDD version 2.6 on 10 instances (10 values of $N \times 2$ values of $V$).  

(m) stated by CÆSAR.BDD version 2.6 on all 20 instances (10 values of $N \times 2$ values of $V$).  

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

(p) safe by construction – stated by the CÆSAR compiler.  

(q) 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).  

(r) 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).  

(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).
## Size of the marking graphs

<table>
<thead>
<tr>
<th>Parameter</th>
<th>Number of reachable markings</th>
<th>Number of transition firings</th>
<th>Max. number of tokens per place</th>
<th>Max. number of tokens per marking</th>
</tr>
</thead>
<tbody>
<tr>
<td>$N = 0, V = a$</td>
<td>$2.4197 e+10$ $(^t)$</td>
<td>?</td>
<td>$1$</td>
<td>$\in [39, 53]$ $(^u)$</td>
</tr>
<tr>
<td>$N = 0, V = b$</td>
<td>$\geq 4.17973 e+13$ $(^v)$</td>
<td>?</td>
<td>$1$ $(^w)$</td>
<td>$\in [2, 53]$ $(^x)$</td>
</tr>
<tr>
<td>$N = 1, V = a$</td>
<td>$1.0858 e+08$ $(^y)$</td>
<td>?</td>
<td>$1$</td>
<td>$\in [43, 57]$ $(^z)$</td>
</tr>
<tr>
<td>$N = 1, V = b$</td>
<td>$\geq 9.64456 e+11$ $(^{aa})$</td>
<td>?</td>
<td>$1$ $(^{ab})$</td>
<td>$\in [2, 57]$ $(^{ac})$</td>
</tr>
<tr>
<td>$N = 2, V = a$</td>
<td>$4.9532 e+09$ $(^ad)$</td>
<td>?</td>
<td>$1$</td>
<td>$\in [43, 57]$ $(^{ae})$</td>
</tr>
<tr>
<td>$N = 2, V = b$</td>
<td>$\geq 2.8490 e+12$ $(^{af})$</td>
<td>?</td>
<td>$1$ $(^{ag})$</td>
<td>$\in [2, 57]$ $(^{ah})$</td>
</tr>
<tr>
<td>$N = 5, V = a$</td>
<td>$2.3099 e+11$ $(^ai)$</td>
<td>?</td>
<td>$1$</td>
<td>$\in [43, 57]$ $(^{aj})$</td>
</tr>
<tr>
<td>$N = 5, V = b$</td>
<td>$\geq 4.4122 e+13$ $(^{ak})$</td>
<td>?</td>
<td>$1$ $(^{al})$</td>
<td>$\in [2, 57]$ $(^{am})$</td>
</tr>
<tr>
<td>$N = 10, V = a$</td>
<td>$\geq 1.6278 e+10$ $(^{an})$</td>
<td>?</td>
<td>$1$ $(^{ao})$</td>
<td>$\in [43, 57]$ $(^{ap})$</td>
</tr>
<tr>
<td>$N = 10, V = b$</td>
<td>$\geq 1.8894 e+13$ $(^{aq})$</td>
<td>?</td>
<td>$1$ $(^{ar})$</td>
<td>$\in [2, 57]$ $(^{as})$</td>
</tr>
<tr>
<td>$N = 20, V = a$</td>
<td>$\geq 2.3660 e+09$ $(^{at})$</td>
<td>?</td>
<td>$1$ $(^{au})$</td>
<td>$\in [43, 57]$ $(^{av})$</td>
</tr>
<tr>
<td>$N = 20, V = b$</td>
<td>$\geq 2.9679 e+12$ $(^{aw})$</td>
<td>?</td>
<td>$1$ $(^{ax})$</td>
<td>$\in [2, 57]$ $(^{ay})$</td>
</tr>
<tr>
<td>$N = 30, V = a$</td>
<td>$\geq 3.4531 e+10$ $(^{az})$</td>
<td>?</td>
<td>$1$ $(^{ba})$</td>
<td>$\in [43, 57]$ $(^{bb})$</td>
</tr>
<tr>
<td>$N = 30, V = b$</td>
<td>$\geq 4.4122 e+13$ $(^{bc})$</td>
<td>?</td>
<td>$1$ $(^{bd})$</td>
<td>$\in [2, 57]$ $(^{be})$</td>
</tr>
<tr>
<td>$N = 40, V = a$</td>
<td>$\geq 6.6539 e+10$ $(^{bd})$</td>
<td>?</td>
<td>$1$ $(^{be})$</td>
<td>$\in [43, 57]$ $(^{bf})$</td>
</tr>
<tr>
<td>$N = 40, V = b$</td>
<td>$\geq 5.7761 e+15$ $(^{bg})$</td>
<td>?</td>
<td>$1$ $(^{bh})$</td>
<td>$\in [2, 57]$ $(^{bi})$</td>
</tr>
<tr>
<td>$N = 50, V = a$</td>
<td>$\geq 7.0293 e+11$ $(^{bh})$</td>
<td>?</td>
<td>$1$ $(^{bj})$</td>
<td>$\in [43, 57]$ $(^{bk})$</td>
</tr>
<tr>
<td>$N = 50, V = b$</td>
<td>$\geq 4.4122 e+13$ $(^{bk})$</td>
<td>?</td>
<td>$1$ $(^{bl})$</td>
<td>$\in [2, 57]$ $(^{bm})$</td>
</tr>
<tr>
<td>$N = 60, V = a$</td>
<td>$\geq 9.4833 e+10$ $(^{bm})$</td>
<td>?</td>
<td>$1$ $(^{bn})$</td>
<td>$\in [43, 57]$ $(^{bo})$</td>
</tr>
<tr>
<td>$N = 60, V = b$</td>
<td>$\geq 5.7761 e+15$ $(^{bn})$</td>
<td>?</td>
<td>$1$ $(^{bp})$</td>
<td>$\in [2, 57]$ $(^{bq})$</td>
</tr>
</tbody>
</table>

$(^t)$ stated by CÆSAR.BDD version 2.6.  
$(^a)$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^v)$ stated by CÆSAR.BDD version 2.6.  
$(^w)$ stated by the CÆSAR compiler.  
$(^y)$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^z)$ stated by CÆSAR.BDD version 2.6.  
$(^u)$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^x)$ stated by the CÆSAR compiler.  
$(^{as})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{ax})$ stated by CÆSAR.BDD version 2.6.  
$(^{ad})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{ae})$ stated by the CÆSAR compiler.  
$(^{af})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{ah})$ stated by CÆSAR.BDD version 2.6.  
$(^{aj})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{al})$ stated by the CÆSAR compiler.  
$(^{am})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{an})$ stated by CÆSAR.BDD version 2.6.  
$(^{ao})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{ar})$ stated by the CÆSAR compiler.  
$(^{as})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{at})$ stated by CÆSAR.BDD version 2.6.  
$(^{au})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{av})$ stated by the CÆSAR compiler.  
$(^{aw})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{ax})$ stated by CÆSAR.BDD version 2.6.  
$(^{ay})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{az})$ stated by the CÆSAR compiler.  
$(^{ba})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bb})$ stated by the CÆSAR compiler.  
$(^{bc})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bd})$ stated by the CÆSAR compiler.  
$(^{be})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bf})$ stated by the CÆSAR compiler.  
$(^{bg})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bh})$ stated by the CÆSAR compiler.  
$(^{bi})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bj})$ stated by the CÆSAR compiler.  
$(^{bk})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bl})$ stated by the CÆSAR compiler.  
$(^{bm})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bn})$ stated by the CÆSAR compiler.  
$(^{bp})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bq})$ stated by the CÆSAR compiler.  
$(^{br})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bs})$ stated by the CÆSAR compiler.  
$(^{bt})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bu})$ stated by the CÆSAR compiler.  
$(^{bv})$ lower and upper bounds given by the number of initial tokens and the number of leaf units.  
$(^{bw})$ stated by the CÆSAR compiler.
lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.

lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.

lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.

lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.

lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.

lower and upper bounds given by the number of initial tokens and the number of leaf units.

stated by CÆSAR.BDD version 2.6.

stated by the CÆSAR compiler.