FORMALIZED MATHEMATICS
Vol. 21, No. 3, Pages 171–184, 2013
DOI: 10.2478/forma-2013-0019

VERSITA
degruyter.com/view/j/forma

Formalization of the Advanced Encryption Standard. Part I[1]

Kenichi Arai[2]
Tokyo University of Science
Chiba, Japan

Hiroyuki Okazaki
Shinshu University
Nagano, Japan

Summary. In this article, we formalize the Advanced Encryption Standard (AES). AES, which is the most widely used symmetric cryptosystem in the world, is a block cipher that was selected by the National Institute of Standards and Technology (NIST) as an official Federal Information Processing Standard for the United States in 2001 [12]. AES is the successor to DES [13], which was formerly the most widely used symmetric cryptosystem in the world. We formalize the AES algorithm according to [12]. We then verify the correctness of the formalized algorithm that the ciphertext encoded by the AES algorithm can be decoded uniquely by the same key. Please note the following points about this formalization: the AES round process is composed of the `SubBytes`, `ShiftRows`, `MixColumns`, and `AddRoundKey` transformations (see [12]). In this formalization, the `SubBytes` and `MixColumns` transformations are given as permutations, because it is necessary to treat the finite field GF(2^8) for those transformations. The formalization of AES that considers the finite field GF(2^8) is formalized by the future article.

MSC: 68P25 94A60 03B35

Keywords: Mizar formalization; Advanced Encryption Standard (AES) algorithm; cryptology

MML identifier: `AESCIP_1`, version: `8.1.02 5.19.1189`

The notation and terminology used in this paper have been introduced in the following articles: [5], [1], [13], [4], [6], [16], [14], [11], [7], [8], [15], [18], [2], [3], [9], [19], [17], and [10].

[1]This work was supported by JSPS KAKENHI 21240001 and 22300285.

[2]This research was presented during the 2012 International Conference on Foundations of Computer Science FCS'12 in Las Vegas, USA.

ISSN 1426–2630(Print), 1898-9934(Online)

1. Preliminaries

Let us consider natural numbers k, m. Now we state the propositions:

(1) If $m \neq 0$ and $(k+1) \bmod m \neq 0$, then $(k+1) \bmod m = (k \bmod m)+1$.

(2) If $m \neq 0$ and $(k+1) \bmod m \neq 0$, then $(k+1) \operatorname{div} m = k \operatorname{div} m$.

(3) If $m \neq 0$ and $(k+1) \bmod m = 0$, then $m-1 = k \bmod m$.

(4) If $m \neq 0$ and $(k+1) \bmod m = 0$, then $(k+1) \operatorname{div} m = (k \operatorname{div} m)+1$.

(5) $(k-m) \bmod m = k \bmod m$.

(6) If $m \neq 0$, then $(k-m) \operatorname{div} m = (k \operatorname{div} m)-1$.

Let m, n be natural numbers, X, D be non empty sets, F be a function from X into $(D^n)^m$, and x be an element of X. Let us observe that the functor $F(x)$ yields an element of $(D^n)^m$. Let m be a natural number, X, Y, D be non empty sets, and F be a function from $X \times Y$ into D^m. Let y be an element of Y. Note that the functor $F(x,y)$ yields an element of D^m. Now we state the propositions:

(7) Let us consider natural numbers m, n, a non empty set D, and elements F_1, F_2 of $(D^n)^m$. Suppose natural numbers i, j. If $i \in \operatorname{Seg} m$ and $j \in \operatorname{Seg} n$, then $F_1(i)(j) = F_2(i)(j)$. Then $F_1 = F_2$.

(8) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4 of D. Then $\langle x_1, x_2, x_3, x_4 \rangle$ is an element of D^4.

(9) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5 of D. Then $\langle x_1, x_2, x_3, x_4, x_5 \rangle$ is an element of D^5.

(10) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of D. Then $\langle x_1, x_2, x_3, x_4 \rangle \frown \langle x_5, x_6, x_7, x_8 \rangle$ is an element of D^8. The theorem is a consequence of (8).

(11) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8, x_9, x_{10} of D. Then $\langle x_1, x_2, x_3, x_4, x_5 \rangle \frown \langle x_6, x_7, x_8, x_9, x_{10} \rangle$ is an element of D^{10}. The theorem is a consequence of (9).

(12) Let us consider a non empty set D and elements x_1, x_2, x_3, x_4, x_5, x_6, x_7, x_8 of D^4. Then $\langle x_1 \frown x_5, x_2 \frown x_6, x_3 \frown x_7, x_4 \frown x_8 \rangle$ is an element of $(D^8)^4$. The theorem is a consequence of (8).

(13) Let us consider a non empty set D, an element x of $(D^4)^4$, and an element k of $\mathbb{N}$. Suppose $k \in \operatorname{Seg} 4$. Then there exist elements x_1, x_2, x_3, x_4 of D such that

(i) $x_1 = x(k)(1)$, and

(ii) $x_2 = x(k)(2)$, and

(iii) $x_3 = x(k)(3)$, and

(iv) $x_4 = x(k)(4)$.

(14) Let us consider non empty sets X, Y, a function f from X into Y, and a function g from Y into X. Suppose

(i) for every element x of X, $g(f(x)) = x$, and

(ii) for every element y of Y, $f(g(y)) = y$.

Then

(iii) f is one-to-one, and

(iv) f is onto, and

(v) g is one-to-one, and

(vi) g is onto, and

(vii) $g = f^{-1}$, and

(viii) $f = g^{-1}$.

2. State Array

The array of AES-State yielding a function from $Boolean^{128}$ into $((Boolean^8)^4)^4$ is defined by

(Def. 1) Let us consider an element i_1 of $Boolean^{128}$ and natural numbers i, j. Suppose $i, j \in \mathrm{Seg}\,4$. Then $it(i_1)(i)(j) = \mathrm{mid}(i_1, (1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32, ((1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32) + 7)$.

Now we state the propositions:

(15) Let us consider a natural number k. Suppose $1 \leqslant k \leqslant 128$. Then there exist natural numbers i, j such that

(i) $i, j \in \mathrm{Seg}\,4$, and

(ii) $(1+(i-'1)\cdot 8)+(j-'1)\cdot 32 \leqslant k \leqslant ((1+(i-'1)\cdot 8)+(j-'1)\cdot 32)+7$.

(16) Let us consider natural numbers i, j, i_0, j_0. Suppose

(i) $i, j, i_0, j_0 \in \mathrm{Seg}\,4$, and

(ii) it is not true that $i = i_0$ and $j = j_0$.

Then $\{k$, where k is a natural number : $(1 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32 \leqslant k \leqslant (8 + (i -' 1) \cdot 8) + (j -' 1) \cdot 32\} \cap \{k$, where k is a natural number : $(1+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32 \leqslant k \leqslant (8+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32\} = \emptyset$.

(17) Let us consider natural numbers k, i, j, i_0, j_0. Suppose

(i) $1 \leqslant k \leqslant 128$, and

(ii) $i, j, i_0, j_0 \in \mathrm{Seg}\,4$, and

(iii) $(1+(i-'1)\cdot 8)+(j-'1)\cdot 32 \leqslant k \leqslant ((1+(i-'1)\cdot 8)+(j-'1)\cdot 32)+7$, and

(iv) $(1+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32 \leqslant k \leqslant ((1+(i_0-'1)\cdot 8)+(j_0-'1)\cdot 32)+7$.

Then

(v) $i = i_0$, and

(vi) $j = j_0$.

The theorem is a consequence of (16).

(18) The array of AES-State is one-to-one. The theorem is a consequence of (15). PROOF: For every elements x_1, x_2 such that x_1, $x_2 \in \mathit{Boolean}^{128}$ and (the array of AES-State)(x_1) = (the array of AES-State)(x_2) holds $x_1 = x_2$ by [15, (3)], [2, (11)], [4, (1)]. □

(19) The array of AES-State is onto. The theorem is a consequence of (15) and (17). PROOF: For every element y such that $y \in ((\mathit{Boolean}^8)^4)^4$ there exists an element x such that $x \in \mathit{Boolean}^{128}$ and y = (the array of AES-State)(x) by [4, (1)], [7, (3)], [15, (3)]. □

Let us note that the array of AES-State is bijective.

Now we state the proposition:

(20) Let us consider an element c of $((\mathit{Boolean}^8)^4)^4$. Then (the array of AES-State)((the array of AES-State)$^{-1}(c)$) = c.

3. `SubBytes`

In this paper S denotes a permutation of $\mathit{Boolean}^8$.

Let us consider S. The functor `SubBytes`(S) yielding a function from $((\mathit{Boolean}^8)^4)^4$ into $((\mathit{Boolean}^8)^4)^4$ is defined by

(Def. 2) Let us consider an element i_1 of $((\mathit{Boolean}^8)^4)^4$ and natural numbers i, j. Suppose i, $j \in \mathrm{Seg}\,4$. Then there exists an element i_2 of $\mathit{Boolean}^8$ such that

(i) $i_2 = i_1(i)(j)$, and

(ii) $\mathit{it}(i_1)(i)(j) = S(i_2)$.

The functor `InvSubBytes`(S) yielding a function from $((\mathit{Boolean}^8)^4)^4$ into $((\mathit{Boolean}^8)^4)^4$ is defined by

(Def. 3) Let us consider an element i_1 of $((\mathit{Boolean}^8)^4)^4$ and natural numbers i, j. Suppose i, $j \in \mathrm{Seg}\,4$. Then there exists an element i_2 of $\mathit{Boolean}^8$ such that

(i) $i_2 = i_1(i)(j)$, and

(ii) $\mathit{it}(i_1)(i)(j) = S^{-1}(i_2)$.

Now we state the propositions:

(21) Let us consider an element i_1 of $((Boolean^8)^4)^4$. Then $(\texttt{InvSubBytes}(S))((\texttt{SubBytes}(S))(i_1)) = i_1$. The theorem is a consequence of (7).

(22) Let us consider an element o of $((Boolean^8)^4)^4$. Then $(\texttt{SubBytes}(S))((\texttt{InvSubBytes}(S))(o)) = o$. The theorem is a consequence of (7).

(23) (i) $\texttt{SubBytes}(S)$ is one-to-one, and

(ii) $\texttt{SubBytes}(S)$ is onto, and

(iii) $\texttt{InvSubBytes}(S)$ is one-to-one, and

(iv) $\texttt{InvSubBytes}(S)$ is onto, and

(v) $\texttt{InvSubBytes}(S) = (\texttt{SubBytes}(S))^{-1}$, and

(vi) $\texttt{SubBytes}(S) = (\texttt{InvSubBytes}(S))^{-1}$.

The theorem is a consequence of (21), (22), and (14).

4. `ShiftRows`

The functor `ShiftRows` yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 4) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and a natural number i. Suppose $i \in \operatorname{Seg} 4$. Then there exists an element x_i of $(Boolean^8)^4$ such that

(i) $x_i = i_1(i)$, and

(ii) $it(i_1)(i) = \text{Op-Shift}(x_i, 5 - i)$.

The functor `InvShiftRows` yielding a function from $((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 5) Let us consider an element i_1 of $((Boolean^8)^4)^4$ and a natural number i. Suppose $i \in \operatorname{Seg} 4$. Then there exists an element x_i of $(Boolean^8)^4$ such that

(i) $x_i = i_1(i)$, and

(ii) $it(i_1)(i) = \text{Op-Shift}(x_i, i - 1)$.

Now we state the propositions:

(24) Let us consider an element i_1 of $((Boolean^8)^4)^4$. Then $\texttt{InvShiftRows}(\texttt{ShiftRows}(i_1)) = i_1$.

(25) Let us consider an element o of $((Boolean^8)^4)^4$. Then $\texttt{ShiftRows}(\texttt{InvShiftRows}(o)) = o$.

(26) (i) `ShiftRows` is one-to-one, and

(ii) `ShiftRows` is onto, and

(iii) `InvShiftRows` is one-to-one, and

(iv) `InvShiftRows` is onto, and

(v) $\texttt{InvShiftRows} = \texttt{ShiftRows}^{-1}$, and

(vi) $\texttt{ShiftRows} = \texttt{InvShiftRows}^{-1}$.

5. AddRoundKey

The functor `AddRoundKey` yielding a function from $((Boolean^8)^4)^4 \times ((Boolean^8)^4)^4$ into $((Boolean^8)^4)^4$ is defined by

(Def. 6) Let us consider elements t_1, k_1 of $((Boolean^8)^4)^4$ and natural numbers i, j. Suppose i, $j \in \operatorname{Seg} 4$. Then there exist elements t_2, k_2 of $Boolean^8$ such that

(i) $t_2 = t_1(i)(j)$, and

(ii) $k_2 = k_1(i)(j)$, and

(iii) $it(t_1, k_1)(i)(j) = \text{Op-XOR}(t_2, k_2)$.

6. Key Expansion

Let us consider S. Let x be an element of $(Boolean^8)^4$.

The functor $\texttt{SubWord}(S, x)$ yielding an element of $(Boolean^8)^4$ is defined by

(Def. 7) Let us consider an element i of $\operatorname{Seg} 4$. Then $it(i) = S(x(i))$.

The functor $\texttt{RotWord}(x)$ yielding an element of $(Boolean^8)^4$ is defined by the term

(Def. 8) $\text{Op-LeftShift}\, x$.

Let n, m be non zero elements of $\mathbb{N}$ and s, t be elements of $(Boolean^n)^m$.

The functor $\texttt{XOR-Word}(s, t)$ yielding an element of $(Boolean^n)^m$ is defined by

(Def. 9) Let us consider an element i of $\operatorname{Seg} m$. Then $it(i) = \text{Op-XOR}(s(i), t(i))$.

The functor `Rcon` yielding an element of $((Boolean^8)^4)^{10}$ is defined by

(Def. 10) (i) $it(1) = \langle \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,1 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0, 0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle \rangle$, and

(ii) $it(2) = \langle \langle 0,0,0,0 \rangle ^\frown \langle 0,0,1,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0, 0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle \rangle$, and

(iii) $it(3) = \langle \langle 0,0,0,0 \rangle ^\frown \langle 0,1,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0, 0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle \rangle$, and

(iv) $it(4) = \langle \langle 0,0,0,0 \rangle ^\frown \langle 1,0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0, 0,0,0 \rangle, \langle 0,0,0,0 \rangle ^\frown \langle 0,0,0,0 \rangle \rangle$, and

(v) $it(5) = \langle\langle 0,0,0,1\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(vi) $it(6) = \langle\langle 0,0,1,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(vii) $it(7) = \langle\langle 0,1,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(viii) $it(8) = \langle\langle 1,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(ix) $it(9) = \langle\langle 0,0,0,1\rangle \frown \langle 1,0,1,1\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$, and

(x) $it(10) = \langle\langle 0,0,1,1\rangle \frown \langle 0,1,1,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle, \langle 0,0,0,0\rangle \frown \langle 0,0,0,0\rangle\rangle$.

Let us consider S. Let m, i be natural numbers and w be an element of $(Boolean^8)^4$. Assume $m = 4$ or $m = 6$ or $m = 8$ and $i < 4 \cdot (7 + m)$ and $m \leqslant i$. The functor $\texttt{KeyExpansionT}(S, m, i, w)$ yielding an element of $(Boolean^8)^4$ is defined by

(Def. 11) (i) there exists an element T_3 of $(Boolean^8)^4$ such that $T_3 = \texttt{Rcon}(\frac{i}{m})$ and $it = \texttt{XOR-Word}(\texttt{SubWord}(S, (\texttt{RotWord}(w))), T_3)$, **if** $i \bmod m = 0$,

(ii) $it = \texttt{SubWord}(S, w)$, **if** $m = 8$ and $i \bmod 8 = 4$,

(iii) $it = w$, **otherwise**.

Let m be a natural number. Assume $m = 4$ or $m = 6$ or $m = 8$. The functor $\texttt{KeyExpansionW}(S, m)$ yielding a function from $((Boolean^8)^4)^m$ into $((Boolean^8)^4)^{4\cdot(7+m)}$ is defined by

(Def. 12) Let us consider an element K of $((Boolean^8)^4)^m$. Then

(i) for every element i of $\mathbb{N}$ such that $i < m$ holds $it(K)(i+1) = K(i+1)$, and

(ii) for every element i of $\mathbb{N}$ such that $m \leqslant i < 4 \cdot (7 + m)$ there exists an element P of $(Boolean^8)^4$ and there exists an element Q of $(Boolean^8)^4$ such that $P = it(K)((i - m) + 1)$ and $Q = it(K)(i)$ and $it(K)(i + 1) = \texttt{XOR-Word}(P, (\texttt{KeyExpansionT}(S, m, i, Q)))$.

The functor $\texttt{KeyExpansion}(S, m)$ yielding a function from $((Boolean^8)^4)^m$ into $(((Boolean^8)^4)^4)^{7+m}$ is defined by

(Def. 13) Let us consider an element K of $((Boolean^8)^4)^m$. Then there exists an element w of $((Boolean^8)^4)^{4\cdot(7+m)}$ such that

(i) $w = (\texttt{KeyExpansionW}(S, m))(K)$, and

(ii) for every natural number i such that $i < 7 + m$ holds $it(K)(i + 1) = \langle w(4 \cdot i + 1), w(4 \cdot i + 2), w(4 \cdot i + 3), w(4 \cdot i + 4)\rangle$.

7. Encryption and Decryption

In the sequel $\mathcal{M}_1$ denotes a permutation of $((Boolean^8)^4)^4$ and $\mathcal{M}_2$ denotes a permutation of $((Boolean^8)^4)^4$.

Let us consider S and $\mathcal{M}_1$. Let m be a natural number, t_1 be an element of $((Boolean^8)^4)^4$, and K be an element of $((Boolean^8)^4)^m$. The functor AES-Cipher$(S, \mathcal{M}_1, t_1, K)$ yielding an element of $((Boolean^8)^4)^4$ is defined by

(Def. 14) There exists a finite sequence s_1 of elements of $((Boolean^8)^4)^4$ such that

(i) $\operatorname{len} s_1 = (7+m)-1$, and

(ii) there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\texttt{KeyExpansion}(S, m))(K)(1)$ and $s_1(1) = \texttt{AddRoundKey}(t_1, K_1)$, and

(iii) for every natural number i such that $1 \leqslant i < (7+m)-1$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\texttt{KeyExpansion}(S, m))(K)(i+1)$ and $s_1(i+1) = \texttt{AddRoundKey}(((\mathcal{M}_1 \cdot \texttt{ShiftRows}) \cdot \texttt{SubBytes}(S))(s_1(i)), K_i)$, and

(iv) there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\texttt{KeyExpansion}(S, m))(K)(7+m)$ and $it = \texttt{AddRoundKey}((\texttt{ShiftRows} \cdot \texttt{SubBytes}(S))(s_1((7+m)-1)), K_n)$.

The functor AES-InvCipher$(S, \mathcal{M}_1, t_1, K)$ yielding an element of $((Boolean^8)^4)^4$ is defined by

(Def. 15) There exists a finite sequence s_1 of elements of $((Boolean^8)^4)^4$ such that

(i) $\operatorname{len} s_1 = (7+m)-1$, and

(ii) there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(1)$ and $s_1(1) = (\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows})(\texttt{AddRoundKey}(t_1, K_1))$, and

(iii) for every natural number i such that $1 \leqslant i < (7+m)-1$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(i+1)$ and $s_1(i+1) = ((\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(\texttt{AddRoundKey}(s_1(i), K_i))$, and

(iv) there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(7+m)$ and $it = \texttt{AddRoundKey}(s_1((7+m)-1), K_n)$.

Now we state the propositions:

(27) Let us consider an element i_1 of $((Boolean^8)^4)^4$. Then ${\mathcal{M}_1}^{-1}(\mathcal{M}_1(i_1)) = i_1$.

(28) Let us consider an element o of $((Boolean^8)^4)^4$. Then $\mathcal{M}_1({\mathcal{M}_1}^{-1}(o)) = o$.

Let us consider a natural number m and an element t_1 of $((Boolean^8)^4)^4$. Now we state the propositions:

(29) $(\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows})((\texttt{ShiftRows} \cdot \texttt{SubBytes}(S))(t_1)) = t_1$.

(30) $((\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(((\mathcal{M}_1 \cdot \texttt{ShiftRows}) \cdot \texttt{SubBytes}(S))(t_1)) = t_1$.

Now we state the propositions:

(31) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements d_k, e_k of $((Boolean^8)^4)^4$. Suppose

(i) $m = 4$ or $m = 6$ or $m = 8$, and

(ii) $d_k = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(1)$, and

(iii) $e_k = (\texttt{KeyExpansion}(S, m))(K)(7 + m)$.

Then $\texttt{AddRoundKey}(\texttt{AddRoundKey}(t_1, e_k), d_k) = t_1$. The theorem is a consequence of (7).

(32) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, an element k_1 of $((Boolean^8)^4)^m$, and elements d_k, e_k of $((Boolean^8)^4)^4$. Suppose

(i) $m = 4$ or $m = 6$ or $m = 8$, and

(ii) $d_k = (\texttt{KeyExpansion}(S, m))(k_1)(1)$, and

(iii) $e_k = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(k_1)))(7 + m)$.

Then $\texttt{AddRoundKey}(\texttt{AddRoundKey}(t_1, e_k), d_k) = t_1$. The theorem is a consequence of (7).

(33) Let us consider a natural number m, elements t_1, o_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements K_1, K_n of $((Boolean^8)^4)^4$. Suppose

(i) $m = 4$ or $m = 6$ or $m = 8$, and

(ii) $K_1 = (\texttt{KeyExpansion}(S, m))(K)(1)$, and

(iii) $K_n = (\mathrm{Rev}((\texttt{KeyExpansion}(S, m))(K)))(7 + m)$, and

(iv) $o_1 = \texttt{AddRoundKey}((\texttt{ShiftRows} \cdot \texttt{SubBytes}(S))(t_1), K_n)$.

Then $(\texttt{InvSubBytes}(S) \cdot \texttt{InvShiftRows})(\texttt{AddRoundKey}(o_1, K_1)) = t_1$. The theorem is a consequence of (32) and (29).

(34) Let us consider natural numbers m, i, an element t_1 of $((Boolean^8)^4)^4$, an element K of $((Boolean^8)^4)^m$, and elements e_i, d_i of $((Boolean^8)^4)^4$. Suppose

(i) $m = 4$ or $m = 6$ or $m = 8$, and

(ii) $i \leqslant (7 + m) - 1$, and

(iii) $e_i = (\texttt{KeyExpansion}(S, m))(K)((7 + m) - i)$, and

(iv) $d_i = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(i + 1)$.

Then $\mathtt{AddRoundKey}(\mathtt{AddRoundKey}(t_1, e_i), d_i) = t_1$. The theorem is a consequence of (7).

(35) Let us consider a natural number m, an element t_1 of $((Boolean^8)^4)^4$, and an element K of $((Boolean^8)^4)^m$. Suppose

(i) $m = 4$, or

(ii) $m = 6$, or

(iii) $m = 8$.

Then $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = t_1$. The theorem is a consequence of (34) and (30). PROOF: Reconsider $N = (7 + m) - 1$ as a natural number. Consider e_s being a finite sequence of elements of $((Boolean^8)^4)^4$ such that $\mathrm{len}\, e_s = N$ and there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathtt{KeyExpansion}(S, m))(K)(1)$ and $e_s(1) = \mathtt{AddRoundKey}(t_1, K_1)$ and for every natural number i such that $1 \leqslant i < N$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathtt{KeyExpansion}(S, m))(K)(i+1)$ and $e_s(i+1) = \mathtt{AddRoundKey}(((\mathcal{M}_1 \cdot \mathtt{ShiftRows}) \cdot \mathtt{SubBytes}(S))(e_s(i)), K_i)$ and there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathtt{KeyExpansion}(S, m))(K)(7 + m)$ and $\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K) = \mathtt{AddRoundKey}((\mathtt{ShiftRows} \cdot \mathtt{SubBytes}(S))(e_s(N)), K_n)$. Consider d_s being a finite sequence of elements of $((Boolean^8)^4)^4$ such that $\mathrm{len}\, d_s = N$ and there exists an element K_1 of $((Boolean^8)^4)^4$ such that $K_1 = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(1)$ and $d_s(1) = (\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows})(\mathtt{AddRoundKey}(\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K), K_1))$ and for every natural number i such that $1 \leqslant i < N$ there exists an element K_i of $((Boolean^8)^4)^4$ such that $K_i = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(i+1)$ and $d_s(i+1) = ((\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows}) \cdot {\mathcal{M}_1}^{-1})(\mathtt{AddRoundKey}(d_s(i), K_i))$ and there exists an element K_n of $((Boolean^8)^4)^4$ such that $K_n = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(7 + m)$ and $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = \mathtt{AddRoundKey}(d_s(N), K_n)$. Consider e_1 being an element of $((Boolean^8)^4)^4$ such that $e_1 = (\mathtt{KeyExpansion}(S, m))(K)(1)$ and $e_s(1) = \mathtt{AddRoundKey}(t_1, e_1)$. Consider e_n being an element of $((Boolean^8)^4)^4$ such that $e_n = (\mathtt{KeyExpansion}(S, m))(K)(7 + m)$ and $\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K) = \mathtt{AddRoundKey}((\mathtt{ShiftRows} \cdot \mathtt{SubBytes}(S))(e_s(N)), e_n)$. Consider d_1 being an element of $((Boolean^8)^4)^4$ such that $d_1 = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(1)$ and $d_s(1) = (\mathtt{InvSubBytes}(S) \cdot \mathtt{InvShiftRows})(\mathtt{AddRoundKey}(\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K), d_1))$. Consider d_n being an element of $((Boolean^8)^4)^4$ such that $d_n = (\mathrm{Rev}((\mathtt{KeyExpansion}(S, m))(K)))(7+m)$ and $\text{AES-InvCipher}(S, \mathcal{M}_1, (\text{AES-Cipher}(S, \mathcal{M}_1, t_1, K)), K) = \mathtt{AddRoundKey}(d_s(N), d_n)$. Define $\mathcal{R}[\text{natural number}] \equiv$ if $\$_1 < N$, then $d_s(\$_1 + 1) = e_s(N - \$_1)$. For every natural number i such that $\mathcal{R}[i]$

holds $\mathcal{R}[i+1]$ by [2, (11)], [15, (3)], [2, (14)]. For every natural number k, $\mathcal{R}[k]$ from [2, Sch. 2]. $\square$

(36) Let us consider a non empty set D, non zero elements n, m of $\mathbb{N}$, and an element r of D^n. Suppose

(i) $m \leqslant n$, and

(ii) $8 \leqslant n - m$.

Then Op-Left(Op-Right$(r, m), 8)$ is an element of D^8.

Let r be an element of *Boolean*^{128}. The functor AES-InitState128Key(r) yielding an element of $((\mathit{Boolean}^8)^4)^4$ is defined by

(Def. 16) (i) $\mathit{it}(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left(Op-Right $(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $\mathit{it}(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $\mathit{it}(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $\mathit{it}(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Right$(r, 120)\rangle$.

Let r be an element of *Boolean*^{192}. The functor AES-InitState192Key(r) yielding an element of $((\mathit{Boolean}^8)^4)^6$ is defined by

(Def. 17) (i) $\mathit{it}(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left(Op-Right $(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $\mathit{it}(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $\mathit{it}(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $\mathit{it}(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Left(Op-Right$(r, 120), 8)\rangle$, and

(v) $\mathit{it}(5) = \langle$Op-Left(Op-Right$(r, 128), 8)$, Op-Left(Op-Right$(r, 136), 8)$, Op-Left(Op-Right$(r, 144), 8)$, Op-Left(Op-Right$(r, 152), 8)\rangle$, and

(vi) $\mathit{it}(6) = \langle$Op-Left(Op-Right$(r, 160), 8)$, Op-Left(Op-Right$(r, 168), 8)$, Op-Left(Op-Right$(r, 176), 8)$, Op-Right$(r, 184)\rangle$.

Let r be an element of *Boolean*^{256}. The functor AES-InitState256Key(r) yielding an element of $((\mathit{Boolean}^8)^4)^8$ is defined by

(Def. 18) (i) $\mathit{it}(1) = \langle$Op-Left$(r, 8)$, Op-Left(Op-Right$(r, 8), 8)$, Op-Left (Op-Right$(r, 16), 8)$, Op-Left(Op-Right$(r, 24), 8)\rangle$, and

(ii) $\mathit{it}(2) = \langle$Op-Left(Op-Right$(r, 32), 8)$, Op-Left(Op-Right$(r, 40), 8)$, Op-Left(Op-Right$(r, 48), 8)$, Op-Left(Op-Right$(r, 56), 8)\rangle$, and

(iii) $it(3) = \langle$Op-Left(Op-Right$(r, 64), 8)$, Op-Left(Op-Right$(r, 72), 8)$, Op-Left(Op-Right$(r, 80), 8)$, Op-Left(Op-Right$(r, 88), 8)\rangle$, and

(iv) $it(4) = \langle$Op-Left(Op-Right$(r, 96), 8)$, Op-Left(Op-Right$(r, 104), 8)$, Op-Left(Op-Right$(r, 112), 8)$, Op-Left(Op-Right$(r, 120), 8)\rangle$, and

(v) $it(5) = \langle$Op-Left(Op-Right$(r, 128), 8)$, Op-Left(Op-Right$(r, 136), 8)$, Op-Left(Op-Right$(r, 144), 8)$, Op-Left(Op-Right$(r, 152), 8)\rangle$, and

(vi) $it(6) = \langle$Op-Left(Op-Right$(r, 160), 8)$, Op-Left(Op-Right$(r, 168), 8)$, Op-Left(Op-Right$(r, 176), 8)$, Op-Left(Op-Right$(r, 184), 8)\rangle$, and

(vii) $it(7) = \langle$Op-Left(Op-Right$(r, 192), 8)$, Op-Left(Op-Right$(r, 200), 8)$, Op-Left(Op-Right$(r, 208), 8)$, Op-Left(Op-Right$(r, 216), 8)\rangle$, and

(viii) $it(8) = \langle$Op-Left(Op-Right$(r, 224), 8)$, Op-Left(Op-Right$(r, 232), 8)$, Op-Left(Op-Right$(r, 240), 8)$, Op-Right$(r, 248)\rangle$.

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{128}$. The functor AES-128enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 19) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2,$ ((the array of AES-State)(m_1)), (AES-InitState128Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-128dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 20) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2,$ ((the array of AES-State)(c)), (AES-InitState128Key(K)))).

Now we state the proposition:

(37) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, and elements m_1, K of $Boolean^{128}$.
Then AES-128dec$(S, \mathcal{M}_2,$ (AES-128enc$(S, \mathcal{M}_2, m_1, K)$)$, K) = m_1$. The theorem is a consequence of (20) and (35).

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{192}$. The functor AES-192enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 21) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2,$ ((the array of AES-State)(m_1)), (AES-InitState192Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-192dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 22) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2,$ ((the array of AES-State)(c)), (AES-InitState192Key(K)))).

Now we state the proposition:

(38) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, an element m_1 of $Boolean^{128}$, and an element K of $Boolean^{192}$.

Then AES-192dec$(S, \mathcal{M}_2, (\text{AES-192enc}(S, \mathcal{M}_2, m_1, K)), K) = m_1$. The theorem is a consequence of (20) and (35).

Let us consider S and $\mathcal{M}_2$. Let m_1 be an element of $Boolean^{128}$ and K be an element of $Boolean^{256}$. The functor AES-256enc$(S, \mathcal{M}_2, m_1, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 23) (The array of AES-State)$^{-1}$(AES-Cipher$(S, \mathcal{M}_2$, ((the array of AES-State)(m_1)), (AES-InitState256Key(K)))).

Let c be an element of $Boolean^{128}$. The functor AES-256dec$(S, \mathcal{M}_2, c, K)$ yielding an element of $Boolean^{128}$ is defined by the term

(Def. 24) (The array of AES-State)$^{-1}$(AES-InvCipher$(S, \mathcal{M}_2$, ((the array of AES-State)(c)), (AES-InitState256Key(K)))).

Now we state the proposition:

(39) Let us consider a permutation S of $Boolean^8$, a permutation $\mathcal{M}_2$ of $((Boolean^8)^4)^4$, an element m_1 of $Boolean^{128}$, and an element K of $Boolean^{256}$.
Then AES-256dec$(S, \mathcal{M}_2, (\text{AES-256enc}(S, \mathcal{M}_2, m_1, K)), K) = m_1$. The theorem is a consequence of (20) and (35).

References

[1] Grzegorz Bancerek. Cardinal numbers. *Formalized Mathematics*, 1(**2**):377–382, 1990.
[2] Grzegorz Bancerek. The fundamental properties of natural numbers. *Formalized Mathematics*, 1(**1**):41–46, 1990.
[3] Grzegorz Bancerek. The ordinal numbers. *Formalized Mathematics*, 1(**1**):91–96, 1990.
[4] Grzegorz Bancerek and Krzysztof Hryniewiecki. Segments of natural numbers and finite sequences. *Formalized Mathematics*, 1(**1**):107–114, 1990.
[5] Czesław Byliński. Binary operations. *Formalized Mathematics*, 1(**1**):175–180, 1990.
[6] Czesław Byliński. Finite sequences and tuples of elements of a non-empty sets. *Formalized Mathematics*, 1(**3**):529–536, 1990.
[7] Czesław Byliński. Functions and their basic properties. *Formalized Mathematics*, 1(**1**): 55–65, 1990.
[8] Czesław Byliński. Functions from a set to a set. *Formalized Mathematics*, 1(**1**):153–164, 1990.
[9] Czesław Byliński. Partial functions. *Formalized Mathematics*, 1(**2**):357–367, 1990.
[10] Czesław Byliński. Some basic properties of sets. *Formalized Mathematics*, 1(**1**):47–53, 1990.
[11] Agata Darmochwał. Finite sets. *Formalized Mathematics*, 1(**1**):165–167, 1990.
[12] U.S. Department of Commerce/National Institute of Standards and Technology. FIPS PUB 197, Advanced Encryption Standard (AES). *Federal Information Processing Standars Publication*, 2001.
[13] Hiroyuki Okazaki and Yasunari Shidama. Formalization of the data encryption standard. *Formalized Mathematics*, 20(**2**):125–146, 2012. doi:10.2478/v10037-012-0016-y.
[14] Andrzej Trybulec. On the decomposition of finite sequences. *Formalized Mathematics*, 5 (**3**):317–322, 1996.
[15] Michał J. Trybulec. Integers. *Formalized Mathematics*, 1(**3**):501–505, 1990.
[16] Wojciech A. Trybulec. Pigeon hole principle. *Formalized Mathematics*, 1(**3**):575–579, 1990.
[17] Zinaida Trybulec. Properties of subsets. *Formalized Mathematics*, 1(**1**):67–71, 1990.

[18] Edmund Woronowicz. Many argument relations. *Formalized Mathematics*, 1(**4**):733–737, 1990.

[19] Edmund Woronowicz. Relations and their basic properties. *Formalized Mathematics*, 1 (**1**):73–83, 1990.

Received October 7, 2013