A Description of Baby Rijndael

ISU CprE/Math 533; NTU ST765-U
February 21, 2005

Baby Rijndael is a scaled-down version of the new AES cipher Rijndael. Since Rijndael was designed in terms of very general algebraic structures, it is quite easy to describe smaller versions of the cipher using similar, but smaller, algebraic constructs. One should note that there is more than one choice (as there is for Rijndael itself) for the precise details of the cipher.

The description given here is not intended to underscore the algebraic principles, but rather to make implementation as easy as possible. Since I've grown rather fond of my baby, I've taken to calling it 'babyrijn' for short.

Block size: The block size for babyrijn is **16 bits.** Usually we think of it as 4 hex digits, $h_0h_1h_2h_3$. Note that h_0 consists of the first four bits of the input stream. However, when h_0 is considered as a hex digit, the first bit is considered the high-order bit.

For example, the input block `1000 1100 0111 0001` would be represented with $h_0 =$`8`, $h_1 =$ `c`, $h_2 =$ `7`, $h_3 =$ `1`.

Key size: The key size is also **16 bits.** We usually write it as 4 hex digits $k_0k_1k_2k_3$.

The state: The steps of the cipher are applied to the state. The state is usually considered to be a 2×2 array of hex digits. However, for the t operation, the state is considered to be an 8×2 array of bits. In converting between the two, each hex digit is considered to be a *column* of 4 bits with the high-order bit at the top.

The input block is loaded into the state by mapping $h_0h_1h_2h_3$ to $\left[\begin{smallmatrix} h_0 & h_2 \\ h_1 & h_3 \end{smallmatrix}\right]$. For example, the input block `1000 1100 0111 0001` would be loaded as

$$\begin{bmatrix} 8 & 7 \\ c & 1 \end{bmatrix} \text{ which, as an } 8 \times 2 \text{ bit matrix is } \begin{bmatrix} 1 & 0 \\ 0 & 1 \\ 0 & 1 \\ 0 & 1 \\ 1 & 0 \\ 1 & 0 \\ 0 & 0 \\ 0 & 1 \end{bmatrix}.$$

The state is usually denoted by **a**.

Number of rounds: Babyrijn consists of several rounds, identical in structure. The default number of rounds is 4. This number is subject to change. Changing the number of rounds affects the overall description of the cipher in a small way and also the key schedule.

The cipher.

At the beginning of the cipher, the input block is loaded into the state as described above and the round keys are computed. The cipher has the overall structure:

$$E(\mathbf{a}) = r_4 \circ r_3 \circ r_2 \circ r_1(\mathbf{a} \oplus \mathbf{k}_0).$$

In this expression, $\mathbf{a}$ denotes the state, $\mathbf{k}_0, \mathbf{k}_1, \mathbf{k}_2, \mathbf{k}_3, \mathbf{k}_4$ the round keys and

$$r_i(\mathbf{a}) = \big(\mathbf{t} \cdot \hat{\sigma}(S(\mathbf{a}))\big) \oplus \mathbf{k}_i,$$

except that in r_4, multiplication by $\mathbf{t}$ is omitted. At the end of the cipher, the state is unloaded into a 16-bit block in the same order as which it was loaded.

Here is a description of the individual components of the cipher.

- The S operation is a table lookup applied to each hex digit of the state:

$$\begin{bmatrix} h_0 & h_2 \\ h_1 & h_3 \end{bmatrix} \xrightarrow{S} \begin{bmatrix} s(h_0) & s(h_2) \\ s(h_1) & s(h_3) \end{bmatrix}$$

where the s function is given by the following table:

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$s(x)$	a	4	3	b	8	e	2	c	5	7	6	f	0	1	9	d

- The $\hat{\sigma}$ operation simply swaps the entries in the second row of the state:

$$\begin{bmatrix} h_0 & h_2 \\ h_1 & h_3 \end{bmatrix} \xrightarrow{\hat{\sigma}} \begin{bmatrix} h_0 & h_2 \\ h_3 & h_1 \end{bmatrix}.$$

- The matrix $\mathbf{t}$ is the following 8×8 matrix of bits:

$$\begin{bmatrix} 1 & 0 & 1 & 0 & 0 & 0 & 1 & 1 \\ 1 & 1 & 0 & 1 & 0 & 0 & 0 & 1 \\ 1 & 1 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 1 & 1 & 1 \\ 0 & 0 & 1 & 1 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 1 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 0 & 1 & 0 & 1 \end{bmatrix}$$

For this transformation, the state is considered to be an 8×2 matrix of bits. The state is multiplied on the left by $\mathbf{t}$ using matrix multiplication modulo 2: $\mathbf{a} \mapsto \mathbf{t} \cdot \mathbf{a}$.

It might be helpful to note that the top left 4×4 submatrix of $\mathbf{t}$ is equal to the bottom right submatrix. And similarly, the top right and bottom left submatrices are equal.

- At the beginning of the cipher and at the end of each round, the state is bitwise added (mod 2) to the round key. The round keys are a 2×2 array of hex digits similar to the state. The *columns* of the round keys are defined recursively as follows:

$$w_0 = \begin{pmatrix} k_0 \\ k_1 \end{pmatrix} \qquad w_1 = \begin{pmatrix} k_2 \\ k_3 \end{pmatrix}$$

$$w_{2i} = w_{2i-2} \oplus S(\text{reverse}(w_{2i-1})) \oplus y_i \qquad w_{2i+1} = w_{2i-1} \oplus w_{2i}$$

for $i = 1, 2, 3, 4$. The constants $y_i = \binom{2^{i-1}}{0}$ and the reverse function interchanges the two entries in the column. The S function is the same one used above. Note that all additions are bit-wise mod 2. Finally, for $i = 0, 1, 2, 3, 4$, the round key $\mathbf{k}_i$ is the matrix whose columns are w_{2i} and w_{2i+1}.

The inverse cipher

The inverse cipher is quite easily deduced from the information given above. Note that the the same round keys are used as for the forward cipher, but in reverse order. The inverse table lookup is

x	0	1	2	3	4	5	6	7	8	9	a	b	c	d	e	f
$s^{-1}(x)$	c	d	6	2	1	8	a	9	4	e	0	3	7	f	5	b

while the inverse of the matrix $\mathbf{t}$ is

$$\begin{bmatrix} 0 & 0 & 1 & 0 & 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 1 & 1 & 0 & 1 & 0 \\ 1 & 1 & 0 & 0 & 1 & 1 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 0 & 1 & 1 \\ 0 & 1 & 0 & 1 & 0 & 0 & 1 & 0 \\ 1 & 0 & 1 & 0 & 1 & 0 & 0 & 1 \\ 1 & 1 & 0 & 1 & 1 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 0 & 0 \end{bmatrix}$$

Example computation

Sample key expansion for key=`6b5d`

$$w_0 = \begin{pmatrix} 6 \\ b \end{pmatrix} \qquad w_1 = \begin{pmatrix} 5 \\ d \end{pmatrix}$$

$$w_1 \xrightarrow{\text{reverse}} \begin{pmatrix} d \\ 5 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} 1 \\ e \end{pmatrix} \oplus w_0 = \begin{pmatrix} 7 \\ 5 \end{pmatrix} \oplus y_1 = \begin{pmatrix} 6 \\ 5 \end{pmatrix} = w_2 \qquad w_1 \oplus w_2 = \begin{pmatrix} 3 \\ 8 \end{pmatrix} = w_3$$

$$w_3 \xrightarrow{\text{reverse}} \begin{pmatrix} 8 \\ 3 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} 5 \\ b \end{pmatrix} \oplus w_2 = \begin{pmatrix} 3 \\ e \end{pmatrix} \oplus y_2 = \begin{pmatrix} 1 \\ e \end{pmatrix} = w_4 \qquad w_3 \oplus w_4 = \begin{pmatrix} 2 \\ 6 \end{pmatrix} = w_5$$

$$w_5 \xrightarrow{\text{reverse}} \begin{pmatrix} 6 \\ 2 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} 2 \\ 3 \end{pmatrix} \oplus w_4 = \begin{pmatrix} 3 \\ d \end{pmatrix} \oplus y_3 = \begin{pmatrix} 7 \\ d \end{pmatrix} = w_6 \qquad w_5 \oplus w_6 = \begin{pmatrix} 5 \\ b \end{pmatrix} = w_7$$

$$w_7 \xrightarrow{\text{reverse}} \begin{pmatrix} b \\ 5 \end{pmatrix} \xrightarrow{S} \begin{pmatrix} f \\ e \end{pmatrix} \oplus w_6 = \begin{pmatrix} 8 \\ 3 \end{pmatrix} \oplus y_4 = \begin{pmatrix} 0 \\ 3 \end{pmatrix} = w_8 \qquad w_7 \oplus w_8 = \begin{pmatrix} 5 \\ 8 \end{pmatrix} = w_9$$

Sample encryption for key=`6b5d` and plaintext block=`2ca5`.

round	**start**	**apply** S	**apply** $\hat{\sigma}$	**mult by t**	$\oplus$	**round key**=	
input	$\begin{bmatrix} 2 & a \\ c & 5 \end{bmatrix}$				$\oplus$	$\begin{bmatrix} 6 & 5 \\ b & d \end{bmatrix}$	=
1	$\begin{bmatrix} 4 & f \\ 7 & 8 \end{bmatrix}$	$\begin{bmatrix} 8 & d \\ c & 5 \end{bmatrix}$	$\begin{bmatrix} 8 & d \\ 5 & c \end{bmatrix}$	$\begin{bmatrix} 2 & f \\ 0 & 7 \end{bmatrix}$	$\oplus$	$\begin{bmatrix} 6 & 3 \\ 5 & 8 \end{bmatrix}$	=
2	$\begin{bmatrix} 4 & c \\ 5 & f \end{bmatrix}$	$\begin{bmatrix} 8 & 0 \\ e & d \end{bmatrix}$	$\begin{bmatrix} 8 & 0 \\ d & e \end{bmatrix}$	$\begin{bmatrix} 0 & a \\ e & 3 \end{bmatrix}$	$\oplus$	$\begin{bmatrix} 1 & 2 \\ e & 6 \end{bmatrix}$	=
3	$\begin{bmatrix} 1 & 8 \\ 0 & 5 \end{bmatrix}$	$\begin{bmatrix} 4 & 5 \\ a & e \end{bmatrix}$	$\begin{bmatrix} 4 & 5 \\ e & a \end{bmatrix}$	$\begin{bmatrix} d & 9 \\ 2 & 8 \end{bmatrix}$	$\oplus$	$\begin{bmatrix} 7 & 5 \\ d & b \end{bmatrix}$	=
4	$\begin{bmatrix} a & c \\ f & 3 \end{bmatrix}$	$\begin{bmatrix} 6 & 0 \\ d & b \end{bmatrix}$	$\begin{bmatrix} 6 & 0 \\ b & d \end{bmatrix}$		$\oplus$	$\begin{bmatrix} 0 & 5 \\ 3 & 8 \end{bmatrix}$	=
output	$\begin{bmatrix} 6 & 5 \\ 8 & 5 \end{bmatrix}$						

Thus the encryption of `2ca5` under key `6b5d` is `6855`.