

A Lightweight Implementation of the Pomaranch S-Box

Cees J.A. Jansen¹, Alexander Kholosha² and Tor Helleseth²

¹ DeltaCrypto B.V.

J.v. Riebeeckstr. 10

5684 EJ Best, The Netherlands

² The Selmer Center

Department of Informatics, University of Norway

P.O. Box 7800, N-5020 Bergen, Norway

9 July 2007

Abstract

The S-box of Pomaranch is defined as a 9-to-7 bits map, where the map consists of taking the inverse modulo $x^9 + x + 1$, and deleting the msb and lsb of the result. In this paper a description of this S-box is given in terms of the inverse in the composite field $GF((2^3)^3)$. It is shown that by choosing an optimal $GF(2^9)$ representation the total gate count of a hardware implementation can be as low as 200 Boolean 2-input gates.

Keywords: S-box, composite field, inverse, irreducible polynomial.

1 Introduction

The stream cipher Pomaranch[1] uses an S-box with 9 bits input and 7 bits output. The S-box is based on the inverse modulo the irreducible polynomial $x^9 + x + 1$ of period 73, with deletion of the most significant and least significant bits of the result.

For implementation in software it suffices to define a table of 512 entries of 7 bits. However, for hardware implementations such a table is not suitable, as multiple copies (8 copies for the 128-bit version of Pomaranch) of the S-box are needed. Moreover, straightforward hardware implementations, based on electronic circuit design programs, typically use input-output relations and therefore result in too complex solutions, i.e. requiring a large number of Boolean gates.

In this paper it is shown how to reduce this complexity by describing the inverse modulo $x^9 + x + 1$ as the inverse in the composite field $GF((2^3)^3)$, i.e. modulo $x^3 + c_1x^2 + c_2x + c_3$, with $c_i \in GF(2^3)$.

This paper is organized as follows. In Section 2 an optimal composite field representation is derived. Section 3 shows the equations involved in taking the direct inverse and their solution. The resulting hardware complexity is discussed in Section 4. Section 5 provides some detailed numerical examples to support hardware implementation. Finally, the paper concludes with Section 6.

2 The composite field representation

The finite field $GF(2^9)$ is commonly represented by elements which are degree eight polynomials. These polynomials are given by their nine binary constants as 9-bit vectors. Addition and multiplication of elements are the componentwise addition modulo 2 (the XOR), and the multiplication of degree-8 polynomials modulo some degree-9 irreducible polynomial $p_1(x)$. The elements are said to be represented in the polynomial basis $B_1 = (\alpha^8, \alpha^7, \dots, \alpha, 1)$, where α is a root of $p_1(x)$, so $p_1(\alpha) = 0$. Note that changing to a different basis $B_2 = (\beta^8, \beta^7, \dots, \beta, 1)$, with $\beta = \alpha^e$, $1 < e < 511$, merely results in a linear transformation of basis, if the minimum polynomial of β has degree nine as well. Consequently, changing the irreducible polynomial $p_1(x)$ into $p_2(x)$ of the same degree, to do the modular multiplications, is realized by a linear transformation.

The field $GF(2^9)$ can also be represented as $GF((2^3)^3)$, where the elements are given as polynomials of degree at most 2 with coefficients from $GF(2^3)$. These field elements can be seen as comprising three times three bits. Addition is again the bitwise modulo 2 addition, but multiplication now becomes the multiplication of two polynomials of degree 2 modulo an irreducible polynomial $q(x)$ of degree three over $GF(2^3)$.

Let α be a primitive element of $GF(2^9)$ with $p(\alpha) = 0$, then it is easy to see ($511 = 7 \cdot 73$) that powers of α^{73} comprise the subfield $GF(2^3)$. Let $\gamma = \alpha^{73}$, then the minimal polynomial of γ is given by

$$r(x) = (x + \gamma)(x + \gamma^2)(x + \gamma^4) = x^3 + (\gamma + \gamma^2 + \gamma^4)x^2 + (\gamma^3 + \gamma^5 + \gamma^6)x + 1$$

As there are only two irreducible polynomials of degree 3 over $GF(2)$, $r(x)$ is either $x^3 + x^2 + 1$ or $x^3 + x + 1$, depending on $p(x)$. Similarly, the minimal polynomial of α with respect to $GF(2^3)$ is given by

$$q(x) = (x + \alpha)(x + \alpha^8)(x + \alpha^{64}) = x^3 + (\alpha + \alpha^8 + \alpha^{64})x^2 + (\alpha^9 + \alpha^{65} + \alpha^{72})x + \alpha^{73}$$

The coefficients of x^2 and x of $q(x)$ are elements of $GF(2^3)$ and, hence, if non-zero can be expressed as powers of γ . The values of the coefficients depend on the primitive polynomial $p(x)$ chosen to define $GF(2^9)$.

In the composite field representation there are two bases involved in representing field elements. There is the basis $(\alpha^2, \alpha, 1)$ to represent elements as vectors of three elements of $GF(2^3)$, and also the basis $(\gamma^2, \gamma, 1)$, with $\gamma = \alpha^{73}$ to represent elements of the subfield $GF(2^3)$ as vectors of three bits. This can be seen as one equivalent basis $B_c = (\alpha^{148}, \alpha^{75}, \alpha^2, \alpha^{147}, \alpha^{74}, \alpha, \alpha^{146}, \alpha^{73}, 1)$ for $GF(2^9)$. Again, a simple linear transformation relates B_c to the polynomial basis B , once $p(x)$ is known.

In general, for calculations involved in determining the inverse modulo some irreducible polynomial it is advantageous to have as many binary values as possible for the coefficients of the polynomial. A simple search through the set of primitive polynomials of degree nine over $GF(2)$ identified the polynomial $x^9 + x^7 + x^5 + x + 1$ as suitable. For if we take $p(x) = x^9 + x^7 + x^5 + x + 1$, then $q(x) = x^3 + x + \gamma$ and $r(x) = x^3 + x + 1$. In this case $((\alpha^7)^9 + \alpha^7 + 1 = 0$, so that $\alpha^7 \mapsto \alpha$ determines the linear transformation mapping polynomials modulo $x^9 + x + 1$ to polynomials modulo $p(x)$. We suffice here by giving the resulting transform matrix \mathbf{M}_{pom} and its inverse, mapping vectors in $GF(2^9)$ defined by $x^9 + x + 1$ to vectors in $GF((2^3)^3)$ defined by $p(x)$ and $\gamma = \alpha^{73}$. Row vector times matrix notation is used.

$$\mathbf{M}_{pom} = \begin{pmatrix} 1 & 1 & 1 & 0 & 0 & 1 & 0 & 1 & 0 \\ 1 & 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 \\ 0 & 0 & 1 & 1 & 0 & 1 & 1 & 1 & 0 \\ 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 1 & 1 & 1 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 1 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 1 & 1 & 0 & 0 & 0 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 1 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}, \mathbf{M}_{pom}^{-1} = \begin{pmatrix} 0 & 0 & 1 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 0 & 0 & 1 & 0 & 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 1 & 0 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 0 & 1 & 0 & 0 & 0 \\ 0 & 1 & 0 & 1 & 0 & 0 & 0 & 1 & 0 \\ 0 & 1 & 1 & 0 & 1 & 0 & 1 & 1 & 0 \\ 1 & 0 & 0 & 1 & 0 & 1 & 1 & 1 & 0 \\ 0 & 1 & 1 & 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 0 & 0 & 0 & 0 & 0 & 1 \end{pmatrix}$$

3 Calculating the inverse

Let $a(x)$ and $b(x)$ be polynomials of degree at most 2 with coefficients from $GF(2^3)$, and let $b(x) = a(x)^{-1} \bmod (x^3 + x + \gamma)$. Given any $a(x)$ it is a straightforward exercise to calculate its inverse $b(x)$: multiply $a(x)$ and $b(x)$ and reduce the powers x^4 and x^3 modulo the irreducible polynomial. The resulting polynomial must be equal to 1 and thus gives rise to a set of three linear equations in three unknowns, that can be solved using Cramer's rules.

$$\begin{aligned} 1 &= (a_2x^2 + a_1x + a_0)(b_2x^2 + b_1x + b_0) \bmod (x^3 + x + \gamma) \\ &= (a_0b_2 + a_2b_0 + a_1b_1 + a_2b_2)x^2 + (a_0b_1 + a_1b_0 + a_1b_2 + a_2b_1 + a_2b_2\gamma)x + \\ &\quad + a_0b_0 + (a_1b_2 + a_2b_1)\gamma \end{aligned}$$

This yields:

$$\begin{pmatrix} a_2 + a_0 & a_1 & a_2 \\ a_2\gamma + a_1 & a_2 + a_0 & a_1 \\ a_1\gamma & a_2\gamma & a_0 \end{pmatrix} \cdot \begin{pmatrix} b_2 \\ b_1 \\ b_0 \end{pmatrix} = \begin{pmatrix} 0 \\ 0 \\ 1 \end{pmatrix}$$

Finally, we obtain:

$$\begin{aligned} D &= (a_2^2\gamma + a_1a_0)(a_2\gamma + a_1) + a_0(a_2 + a_0)^2 + a_1^3\gamma \\ b_2 &= (a_1^2 + a_2(a_2 + a_0))D^{-1} \\ b_1 &= (a_2^2\gamma + a_1a_0)D^{-1} \\ b_0 &= ((a_2 + a_0)^2 + a_1(a_2\gamma + a_1))D^{-1} \end{aligned}$$

The above results have been written in a form that allows reuse of calculated intermediate values. The calculations are carried out in $GF(2^3)$, with γ primitive element, satisfying $\gamma^3 + \gamma + 1 = 0$.

4 Hardware implementation

All calculations are done in $GF(2^3)$, where elements are represented in the polynomial basis $(\gamma^2, \gamma, 1)$. Hence, the field elements are $(0, 1, \gamma, \gamma^2, \dots, \gamma^6)$, corresponding to the vectors $(000, 001, 010, 100, 011, 110, 111, 101)$. This means that all operations on single field elements are implemented as three Boolean functions of three binary variables. The multiplication is realized with three Boolean functions of six binary variables. Clearly, addition is realized with three XORs. The following table shows the functions that are realized and their (2-input Boolean) gate complexities (rightmost column).

$y = x^{-1}$	$y_0 = x_0 + (x_1 \vee x_2)$ $y_1 = x_0x_1 + x_2$ $y_2 = x_1 + \bar{x}_0x_2$	6
$y = x \cdot \gamma$	$y_0 = x_2$ $y_1 = x_0 + x_2$ $y_2 = x_1$	1
$y = x^2$	$y_0 = x_0$ $y_1 = x_2$ $y_2 = x_1 + x_2$	1
$y = x^3 \cdot \gamma$	$y_0 = x_0x_1 + x_2$ $y_1 = (x_0 \vee x_2) + x_1x_2$ $y_2 = (x_0 \vee x_2) + x_0\bar{x}_2$	7
$z = x \cdot y$	$z_0 = x_0y_0 + x_1y_2 + x_2y_1$ $z_1 = x_0y_1 + x_1y_0 + x_1y_2 + x_2y_1 + x_2y_2$ $z_2 = x_0y_2 + x_2y_0 + x_1y_1 + x_2y_2$	17

To calculate D we need 3 multiplications, two squares, five additions, two multiplications by γ and one $x^3 \cdot \gamma$ operation, for a total of 77 Boolean gates. Calculation of D^{-1} requires 6 gates. To calculate b_2, b_1, b_0 another $38 + 17 + 37 = 92$ gates are required, bringing the total number of gates to 175.

The linear transformation \mathbf{M}_{pom} and its inverse also require XOR-gates. Their complexity is small, however, if they are implemented by using partial sums, as illustrated below:

$$\mathbf{M}_{pom} : \begin{cases} p_1 = x_8 + x_2 \\ p_2 = x_6 + x_4 \\ y_8 = p_1 + x_7 + x_5 + x_3 \\ y_7 = p_1 + x_4 \\ y_6 = y_8 + p_2 \\ y_5 = y_1 + x_8 + x_3 \\ y_4 = x_7 + x_4 \\ y_3 = x_8 + x_7 + x_6 + x_1 \\ y_2 = y_6 + x_8 \\ y_1 = y_3 + x_4 \\ y_0 = x_0 \end{cases}, \mathbf{M}_{pom}^{-1} : \begin{cases} p = y_8 + y_4 \\ x_8 = y_6 + y_2 \\ x_7 = x_4 + y_4 \\ x_6 = x_4 + y_8 + y_6 \\ x_5 = x_3 + p + y_7 \\ x_4 = y_3 + y_1 \\ x_3 = x_8 + y_5 + y_1 \\ x_2 = x_8 + x_4 + y_7 \\ x_1 = p + y_3 + y_2 \\ x_0 = y_0 \end{cases}.$$

The total number of gates for the linear transformations equals 29 when using the illustrated implementation.

The fact that the msb and lsb of the output are not needed, reduces the gate count by 1 XOR in the inverse linear transformation and 4 gates in the final multiplication of b_0 . This brings the total number of gates for this implementation of the Pomaranch S-box to 199 gates.

5 Numerical examples

To facilitate implementation two numerical examples are given. First example.

$$x \hat{=} (000000010) \xrightarrow{\mathbf{M}_{pom}} (000101010) \hat{=} \gamma^6 x + \gamma$$

$$a_2 = (000), a_1 = (101), a_0 = (010)$$

$$h_1 = a_2^2 \gamma + a_1 a_0 = 1 \quad (001)$$

$$h_2 = a_2 \gamma + a_1 = \gamma^6 \quad (101)$$

$$h_3 = a_2 + a_0 = \gamma \quad (010)$$

$$D = h_1 h_2 + a_0 h_3^2 + a_1^3 \gamma = \gamma^6 + \gamma^3 + \gamma^5 = 1 \quad (001) \longrightarrow D^{-1} = 1 \quad (001)$$

$$b_2 = (a_1^2 + a_2 h_3) D^{-1} = \gamma^5 \quad (111)$$

$$b_1 = h_1 D^{-1} = 1 \quad (001)$$

$$b_0 = (h_3^2 + a_1 h_2) D^{-1} = \gamma^3 \quad (011)$$

$$\gamma^5 x^2 + x + \gamma^3 \hat{=} (111001011) \xrightarrow{M_{\text{pom}}^{-1}} (100000001) \hat{=} x^8 + 1$$

Second example.

$$x^8 + x^6 + x^4 + x^2 + 1 \hat{=} (101010101) \xrightarrow{M_{\text{pom}}} (010010111) \hat{=} \gamma x^2 + \gamma x + \gamma^5$$

$$a_2 = (010), a_1 = (010), a_0 = (111)$$

$$h_1 = a_2^2 \gamma + a_1 a_0 = \gamma^4 \quad (110)$$

$$h_2 = a_2 \gamma + a_1 = \gamma^4 \quad (110)$$

$$h_3 = a_2 + a_0 = \gamma^6 \quad (101)$$

$$D = h_1 h_2 + a_0 h_3^2 + a_1^3 \gamma = \gamma + \gamma^3 + \gamma^4 = \gamma^5 \quad (111) \longrightarrow D^{-1} = \gamma^2 \quad (100)$$

$$b_2 = (a_1^2 + a_2 h_3) D^{-1} = \gamma \quad (010)$$

$$b_1 = h_1 D^{-1} = \gamma^6 \quad (101)$$

$$b_0 = (h_3^2 + a_1 h_2) D^{-1} = 0 \quad (000)$$

$$\gamma x^2 + \gamma^6 x \hat{=} (010101000) \xrightarrow{M_{\text{pom}}^{-1}} (011011010) \hat{=} x^7 + x^6 + x^4 + x^3 + x$$

In the examples above the leftmost and the rightmost bits of the results must be discarded in order to obtain the corresponding Pomaranch S-box outputs. Indeed, entry 2 of the S-box table contains the value 0 and entry 341 contains the value 109.

6 Conclusions

This paper shows that the Pomaranch S-box can be implemented with as few as 200 Boolean 2-input gates by applying the composite field representation of the field $GF(512)$. It should be noted that these results might even be improved by using normal basis representations.

The results of this paper should facilitate the hardware implementation of Pomaranch version 3. One section of this stream cipher can be realized with some 400 gates (200 for the last section which has no S-box), bringing the total gate count to 3400 gates for the 128-bit version and 2200 gates for the 80-bit version.

References

- [1] Jansen, C.J.A., Hellesteth, T., Kholosha, A.: Cascade Jump Controlled Sequence Generator and Pomaranch Stream Cipher (Version 3)". eSTREAM, ECRYPT Stream Cipher Project, Report 2006/006 (2006) <http://www.ecrypt.eu.org/stream/papers.html>.