



VLSI Design & Consultancy

DATASHEET

**Galois Field Multiplier Generator
Version 1.0**

Disclaimer

This document is written in good faith with the intend to assist the readers in the use of the product. Circuit diagrams and other information relating to Think Silicon Ltd products are included as a means of illustrating typical applications. Although the information has been checked and is believed to be accurate, no responsibility is assumed for inaccuracies. Information contains in this document is subject to continuous improvements and developments.

Think Silicon Ltd products are not designed, intended, authorized or warranted for use in any life support or other application where product failure could cause or contribute to personal injury or severe property damage. Any and all such uses without prior written approval of Think Silicon Ltd. will be fully at the risk of the customer.

Think Silicon Ltd. disclaims and excludes any and all warranties, including without limitation any and all implied warranties of merchantability, fitness for a particular purpose, title, and infringement and the like, and any and all warranties arising from any course or dealing or usage of trade.

This document may not be copied, reproduced, or transmitted to others in any manner. Nor may any use of information in this document be made, except for the specific purposes for which it is transmitted to the recipient, without the prior written consent of Think Silicon Ltd. This specification is subject to change at anytime without notice. Think Silicon Ltd. is not responsible for any errors contained herein.

In no event shall Think Silicon Ltd. be liable for any direct, indirect, incidental, special, punitive, or consequential damages; or for lost of data, profits, savings or revenues of any kind; regardless of the form of action, whether based on contract; tort; negligence of Think Silicon Ltd or others; strict liability; beach of warranty; or otherwise; whether or not any remedy of buyers is held to have failed of its essential purpose, and whether or not Think Silicon Ltd. has been advised of the possibility of such damages.

Copyright Notice

No part of this specification may be reproduced in any form or means, without the prior written consent of Think Silicon Ltd.

Questions or comments may be directed to:

Think Silicon Ltd
Suite B12
Patras Science Park
Rion Achaïas 26504
Greece

web: <http://www.think-silicon.com>
email: info@think-silicon.com
Tel: +30 2610 911543

1 Overview

The Think-Silicon *Galois Field Multiplier Generator* is a web configurable Galois Field Multiplier generator.

2 Features

- Easy to use Graphical Web User Interface
- Fully Parallel Combinatorial Implementation of Galois Field Multiplier
- Hardware Acceleration due to Parallel Implementation
- Suitable for
 - Encryption: AES, AES-GCM
 - Elliptic Curve Cryptography (ECC) Algorithms: ECDSA, ECDH
 - Forward Error Correction (FEC) Codes: Reed Solomon, BCH codes
- Multiplication over the extension Galois Field $GF(2^m)$, for any integer $m > 1$.
- User defined primitive polynomial degree for defining the extension Galois Field $GF(2^m)$
- User defined polynomial coefficients for defining the extension Galois Field $GF(2^m)$
- Verilog™¹ HDL synthesizable RTL code

3 Architecture

3.1 Port Diagram

Figure 3-1 represents the basic Port Diagram of *GF_mult* component, generated by the *Galois Field Multiplier Generator* toolkit. *GF_mult* performs multiplication over the extension Galois Field $GF(2^m)$ of the multiplicand $a[m-1:0]$ by the multiplier $b[m-1:0]$ and produces the product $z[m-1:0]$. m corresponds to the degree of the primitive polynomial that defines the extension Galois Field $GF(2^m)$.

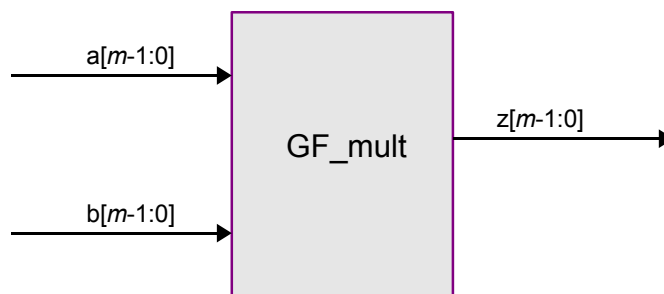


Figure 3-2 Galois Field Multiplier Port Diagram

3.2 Port Interface

Table 3-1 shows the port signals of the *GF_mult* component. m corresponds to the degree of the primitive polynomial that defines the extension Galois Field $GF(2^m)$.

Table 3-1 Port Interface of *GF_mult*

PORT	TYPE	DESCRIPTION
$a[m-1:0]$	Input	The m -bit wide polynomial representation of the multiplicand. $a[m-1]X^{(m-1)} + a[m-2]X^{(m-2)} + \dots + a[1]X + a[0]$

¹ Verilog is a trademark of Cadence Design Automation. (<http://www.cadence.com>)

PORT	TYPE	DESCRIPTION
b[m-1:0]	Input	The m -bit wide polynomial representation of the multiplier. $b[m-1]X^{(m-1)} + b[m-2]X^{(m-2)} + \dots b[1]X + b[0]$
z[m-1:0]	Output	The m -bit wide polynomial representation of the result. $z[m-1]X^{(m-1)} + z[m-2]X^{(m-2)} + \dots z[1]X + z[0]$

Note: 1. $X, X^2, \dots, X^{m-2}, X^{m-1}$ are the basis elements of the $GF(2^m)$ polynomial representation
 2. All representations concerning Galois Field arithmetic are done throughout this document in the standard basis

4 Generator usage

The Galois Field Multiplier Generator employs a graphical web user interface (GUI) for configuring and generating the multiplier component *GF_mult*. In order to use the GUI you must sign-in Think Silicon Ltd web site. If already registered, click on *Sign-in* link in the upper, right side of the web page. Otherwise click on *Register* link first and follow the instructions.

In initial GUI page is shown in Figure 4-1 the user can set the *Polynomial Degree* parameter which corresponds to the degree (m) of the primitive polynomial that defines the extension Galois Field $GF(2^m)$.



Figure 4-1 The primitive polynomial degree selection screen

On the next screen (Figure 4-1), the user can select the coefficients of the m -degree primitive polynomial

$$g(X) = g[m]X^m + g[m-1]X^{(m-1)} + g[m-2]X^{(m-2)} + \dots g[1]X + g[0] \tag{1}$$

that defines the extension Galois Field $GF(2^m)$. The $g[m], g[m-1], g[m-2], g[0]$ coefficients may be either 1 or 0. A tick in a box corresponds to 1 and an empty box corresponds to 0. $g[m]$ is always preselected and set to 1.

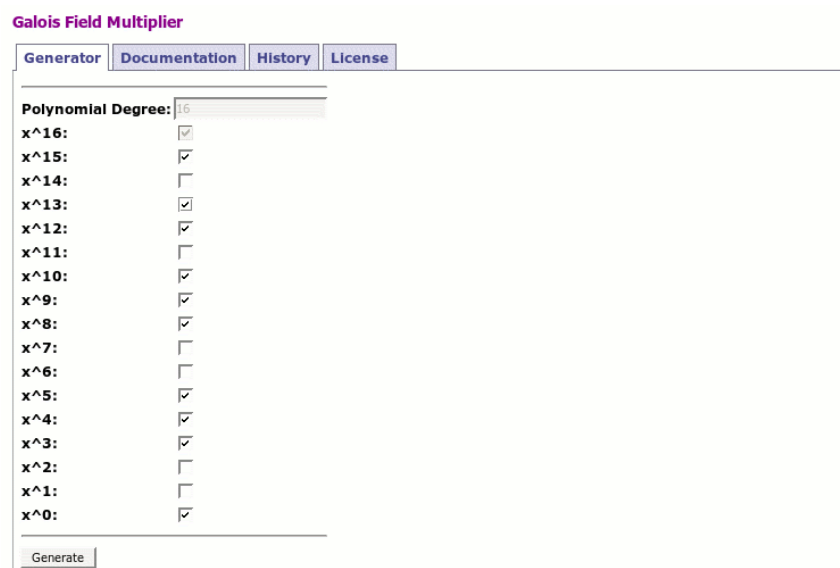


Figure 4-1 The primitive polynomial coefficients selection screen

Note: User defined polynomial coefficients should correspond to a primitive polynomial

5 Deliverables

The Galois Field Multiplier Generator deliverables package consists of the files listed in Table 5-1.

Table 5-1 *Galois Field Multiplier Generator* Deliverables

File	Description
GF_mult.v	<i>GF_mult</i> Verilog™ HDL RTL code
parameters.txt	<i>Galois Field Multiplier</i> configuration parameters
TSi_GF_mult.pdf	The present document