Philips Crypto

GCD-Φ General Crypto Device

Highly secure, programmable encryption engine

A powerful, high-speed programmable cryptographic engine handling private key and public key cipher systems, GCD-Φ offers efficient implementation of all common standard and customer-specific algorithms. With a programmable 32-bit RISC arithmetic processor, this highly integrated device performs a full range of dedicated cryptographic functions including data encryption/decryption, key generation, and storage and management of key data, while delivering outstanding encryption rates - up to 100 Mbits/s.

Key features and functions

- **Application specific hardware including a 32-bit arithmetic processor**
- **RAM controller with 32 kbit memory for arithmetic processor software and data**
- **Software-controlled, 8051-compatible 8-bit microcontroller**
- **I/O-control module**
- **Random number generator**
- **Handles all standard algorithms (DES, IDEA, RSA and SHA) and customer-specific algorithms**
- **Data encryption, decryption, hashing and authentication**
- **Modular and long integer arithmetic operations**
- **Block transformation operations**
- **Internal storage of keys, data and programs**
- **Security interface functions**

A CMOS ASIC, the GCD family is based on technology proven in governmental and industrial applications, incorporating secure memory management to prevent external access to the key data and storing intermediate results on-chip. The arithmetic processor includes a 128-bit hyper-secure memory, only accessible via special instructions and which can be instantly erased in an emergency - even in battery back-up mode.

Providing functionality for long integer arithmetic and substitution functions, the arithmetic processor also incorporates an encryption core for high-speed encryption using a programmable algorithm. This algorithm, together with key and program data, is stored in the on-chip 32 kbit RAM.

Integrity *starts here*

Let's make things better.

PHILIPS

Facilitating hardware and software design

Test board

Enabling designers to test the full functionality of the GCD-Φ, the test board supports the chip's complete configuration capabilities, with all the pins connected to test pins. A four layer board, it comes with a detailed Application Note and it includes an on-board lithium battery so requires only a 7V - 10V/500 mA DC power supply.

Integrated Development Environment (IDE)

This comprehensive software development environment includes an editor, assembler, debugging facilities and a software simulator (APSIM) for the arithmetic processor.

Offering a full range of standard editing features, the editor also supports debugging functions such as breakpoints and watches. The debugger provides simple run control through features including single step and go/continue operation. Further debugging information is supplied by the integrated assembler which displays errors and warnings in a separate, dedicated message window, with the corresponding source code lines indicated in the editor window.

The APSIM allows developers to set watches on the contents of both memory and registers, and also includes an I/O simulator.

The GCD-Φ features in full

- **Monolithic ASIC CMOS 3.3 V device**
- **On-chip cryptographic functions:**
  - **secure key storage**
  - **key management**
  - **multiple algorithm capability**
  - **variable width block transformations**
  - **bit permutations**
  - **random number generator**
- **32-bit arithmetic processor handles:**
  - **modular and long integer functions**
  - **digital signature identification protocols**
  - **key and prime number generation**
  - **proprietary cryptographic algorithms**
  - **proprietary public key algorithms**
  - **block cipher functions (64-bit to 160-bit blocks)**
  - **stream cipher functions**
- **Arithmetic processor includes 128-bit hyper-secure memory, with emergency erase function**
- **Software-controlled 8051 microcontroller with external 64 K ROM and 64 K RAM for user applications**
- **32 kbit internal RAM includes battery back-up for storage of programs, keys and sensitive data**
- **Secure memory management logic with separate read and write access**
- **Flexible interface functions:**
  - **data port: 32-bit bi-directional, 16-bit and 8-bit uni-directional/bi-directional register, high-speed synchronous and asynchronous mode**
  - **user interface: 3 multi-purpose control/communication ports**
  - **external controller mode**
- **5 V compliant I/O**
- **48 MHz main system clock**
- **On-chip clock oscillator for external crystal**
- **TQFP144 package**

Specialist documentation, User Group and consultancy support

Secure Non-Disclosure Agreement

GCD-Φ represents proven encryption technology already in use in sensitive applications and Philips Crypto requires any interested company to sign a Non-Disclosure Agreement (NDA). Detailed information such as the chip specification cannot be obtained until this agreement has been officially completed and signed by an authorized person.

Comprehensive application notes

Once an NDA has been signed, customers interested in using the GCD-Φ have access to full information on the device, including the chip specification and a number of application notes. In particular, notes are available on the different encryption algorithms such as DES and Triple DES, and their implementation on the GCD-Φ.

User Group for information exchange

To help customers take full advantage of the potential of this flexible, high-performance device - and to help ensure security and confidentiality - GCD-Φ users join a dedicated User Group. Managed by Philips Crypto and meeting twice a year, this group provides a forum where customers can share their knowledge and experience, and members receive product information and news, datasheets and application notes, updates and occasional newsletters - at no additional cost. And by subscribing to the User Group, users also have a unique opportunity to influence the development of future generations of the GCD-Φ family. Typically, User Group members are system integrators active in the field of data security for banking, government, e-commerce, computer networking and other sectors where confidentiality is of the utmost importance.

Consultancy and custom design

With a wealth of experience and know-how built-up over its 40 year history in cryptography, Philips Crypto supports customers with expert assistance in application development. This expertise goes beyond hardware design, also covering the co-development of custom software libraries, if required.

Integrity *starts here*

Philips Crypto: long experience and future commitment

GCD-Φ underlines Philips Crypto's commitment to helping customers incorporate the very latest advances in encryption into their own applications. Already a second generation chip, a successor to the proven GCD, the GCD-Φ is part of an ongoing development program for powerful, programmable encryption devices.

Philips Crypto is now collaborating with other leading specialists in cryptography to develop a next generation device which will offer even higher speeds with lower power demands. As part of the global Philips' Electronics organization, Philips Crypto has access to vast resources for this and future developments, including the specialist expertise of Philips Research, one of the largest privately-funded research organizations in the world. With joint research programs into emerging standards and enhanced algorithms, Philips Crypto will continue to meet market demands for ever greater security and performance.

The GCD-Φ crypto engine proven in real products

Benefiting from Philips Crypto's long experience, the GCD-Φ crypto engine is at the heart of a number of Philips Crypto products providing highly sophisticated, cost-effective protection for computer networks and personal computers.

Virtual Private Network Guard (VPN Guard)

The VPN Guard system protects Local Area Networks (LANs) against unauthorized access, through Guard devices placed at the LAN side of the router connecting the network to the public network (the Wide Area Network - WAN). Secure communication is guaranteed through a Security Management System which handles all aspects of encryption key management.

VKaart

VKaart is designed to limit access to personal computers and data held on central file servers via smart cards and passwords. Highly configurable and with multi-level security, this user-friendly system offers high-speed hardware-based file encryption and security logging, enabling large groups of users to share data securely.

2 Mbit Link Encryption System (LES)

Philips Crypto's 2 Mbit LES is designed to stop intruders 'listening-in' on data transmissions over leased lines by encrypting all transmissions where communication is protected in the physical layer (Layer 1) of the network.

GCD-Φ is a high-technology encryption device and subject to the export control laws and regulations of the Netherlands. Philips' policy is to comply strictly with all relevant laws and regulations.

Philips Crypto

Philips Crypto BV

Building BAH

De Witbogt 2

P.O. Box 218

5600 MD Eindhoven

the Netherlands

Tel: +31 40 2722600

Fax: +31 40 2723658

E-mail: info@crypto.philips.com

www.crypto.philips.com

12NC: 9922 154 22011

Let's make things better.

PHILIPS

PHILIPS