Development of P2ROM™ with Embedded Gate Arrays

Yoshimasa Sekino Hiroyuki Fukuyama

Nonvolatile memory is used as a device for storing data and programs in a variety of applications. Because of its nonvolatile characteristics, its representative applications are the storage of data, such as boot programs for system start up, electronic dictionaries or memory cards.

Customized specifications have been required in recent years involving individually unique interface functions or added specialized functions, due to the sophistication of user systems. This is because specifications suitable to further sophisticate systems or emphasize performances are different for each user.

A P2ROM™*1) with embedded gate arrays was recently developed in order to facilitate an easier realization of customized specifications. Mix loading gate arrays make it possible to assimilate the design of segments with customized specifications with the design of application specific integrated circuits (ASIC). The embedded gate array chip that we developed and the examination of its application example conducted for the ROM used in memory cards are suitable for personal information protection by loading robust security functions, which is an issue of great concern particularly in recent years.

What a P2ROM™ Is

A P2ROM™ is a unique product of Oki Electric with a business model that involves the shipping of devices completed through the assembly process after writing user data in the test process.

In general, nonvolatile memories are classified into rewritable-types of memories represented by flash memories and non-rewritable-types of memories represented by mask ROM. Memories that can be rewritten are often used in applications involving the storage of data with temporary storage media used in digital cameras and portable audio devices as their competent field. Memories that cannot be rewritten are often used in applications involving the provision of prerecorded data with media, such as electronic dictionaries and memory cards that do not need to be rewritten as their competent field. The P2ROM™ belongs to the non-rewritable memory-type used for electronic dictionaries and memory cards when the differentiation of these products is realized through a business model.

Differentiation of products is possible through the selection of a method used for storing data in the case of nonvolatile memories intended for the provision of data. Since data is written in mask ROMs during the wafer process a mask is created with data that has been supplied by the user and the product will finally be shipped only after going through the wafer, assembly and the test processes. Therefore, a lead time of anywhere from a few weeks to a month or so will be required from the time the data is obtained to the shipping of products and expenses will also be incurred relating to the creation of a mask.

However, it is possible to ship products out in the shortest possible time of two days after data has been obtained with the P2ROM™. This is realized by taking advantage of the feature of the P2ROM™, which is a device that can be electronically written only once. Data supplied by users is electronically written into the final process of the production, the test process, thereby making it possible to reduce the time required from the acquisition of data to the shipping of products.

Shipping with a minimum delivery time is advantageous also because the user can maintain a minimum quantity of products in their inventory. Furthermore, it is advantageous for the user if the user is developing a product as the corrections to their data can be implemented in a speedy manner. Efficient inspections are possible since it is possible to obtain a modified version in just a few days and then continue with the verification process when the correction of data becomes necessary during an evaluation with actual equipment. This is also an advantage that makes it possible to perform debugging work until immediately before the evaluation with actual equipment that requires the P2ROM™.

Need for Embedded Gate Arrays

In order to realize customized specifications, which are becoming larger in scale and more complex in content, in a short development period, it is essential to implement the ASIC design methodology. The functions developed by users using the ASIC design can be adopted, thereby achieving a heightened added value.

When developing a new electronic device, the shortening of the development period becomes an important design issue. Since products with customized specifications are intended for a particular user, some products may not have any commercial value unless the delivery date required by the user can be attained. For this reason achieving the delivery date becomes the foremost premise and the shortening of the development time becomes important.

*1) P2ROM is a trademark of Oki Electric Industry Co., Ltd.

For memory LSIs, such as the P2ROM™ and others, not only are inverter circuits and logical circuits, including AND circuits, in use but also many circuits designed on transistor levels as well as analog circuits. For this reason both the circuit design and pattern design become manual procedures, as is the design of customized specifications, which is also performed using manual procedures.

Conventional customized specifications were usually modifications that involved simple changes, such as the partial improvement of existing functions or an addition of simple functions to interface specifications presenting little impact on the development period even when they were conducted by manually implementing design procedures. In recent years, however, complex functional requirements, such as the implementation of command-type interfaces and processing of read data, are on the increase. For this reason, manually implemented design procedures require a staggering amount of work, which causes a problem by increasing the development time.

In order to perform customized specifications on a larger scale and more complex designs in a shorter period of time, we decided to embed gate arrays and adopt the ASIC design methodology. Although estimates vary depending on the functions the estimate for the development period using the ASIC design methodology has reduced the time to approximately one-third or less in comparison with manually implemented designs.

Furthermore, the adoption of functions designed by the user's ASIC designs also became possible even though it was not possible with manually implemented designs.

Embedded Gate Array Chips and Their Applications

A chip image of the chip with embedded gate arrays developed recently is shown in **Figure 1**. The gate array is positioned between the P2ROM™ memory core and the input/output circuit.

A control method involving the logic circuit in the gate array section performing the overall control of the chip was adopted for the chip prototyped recently. The externally input signal is input in the gate array via the input/output circuit. Memory core control signals and data output control signals are generated by the gate array, in accordance with input signals. The memory cell core performs data reading operations according to the control signal and the read data is transmitted to the input/output circuit via the gate array. The input/output circuit section outputs data according to the data output control signal.

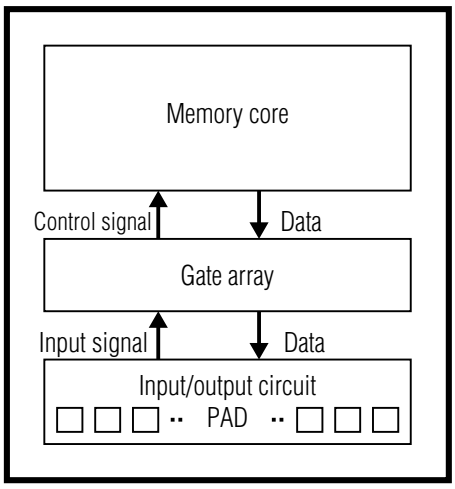

Fig. 1 Chip image

Security functions causing heightened concern in recent years are examples of the type of applications for command-type interfaces and read data processing functions. Sophisticated security functions require complex encryption technologies, which contribute to the problem of increasing development periods. The effectiveness of application devices with the chips with embedded gate array can be expected since using the ASIC design method can shorten the development period.

Encryption Technology

Security issues regarding information can be summarized into the following three aspects. The first is the issue of referencing, intercepting and viewing information through unauthorized means, the second is the issue of tampering involving the modification of data content belonging to other people and the third is the issue of impersonation involving other parties pretending to be the parties concerned. The encryption technology is an extremely important technology as a

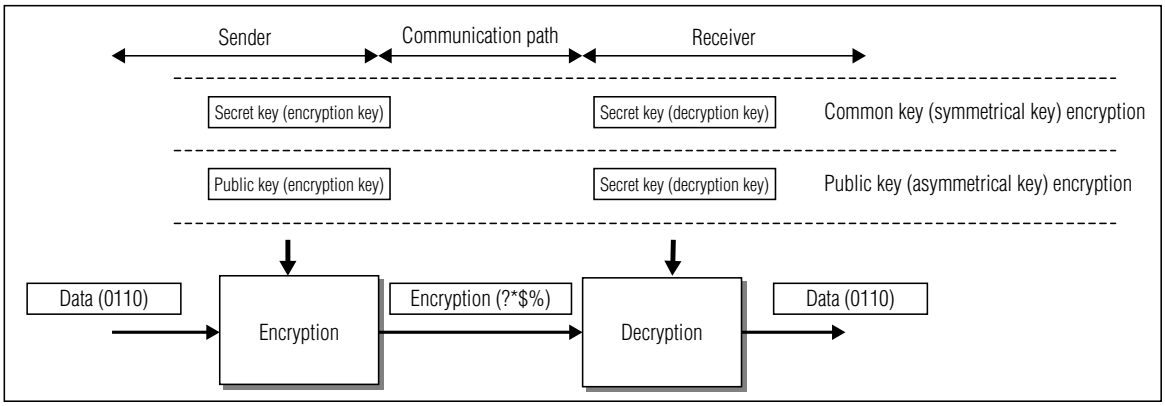

Fig. 2 Encryption methods

countermeasure for such security issues.

A conceptual diagram of the encryption method is shown in **Figure 2**. There are two encryption methods available, the common key encryption method and the public key encryption method. The common key encryption method uses one key (a common key) for the encryption and decryption of information. Since this is an extremely simple method, it is possible to provide it in a compact manner and also at a high-speed. The public key encryption method, on the other hand, uses two keys for the encryption and decryption of information. One of these keys is called a public key, while the other is called a secret key. Disclosure of the public key would not cause a problem, since data encrypted using a public key can only be decrypted using a secret key.

Encryption of Memory Data

As described at the beginning of the paper, the P2ROM™, a nonvolatile memory, is often used as a storage media for information used in electronic dictionaries and memory cards. Information recorded in these applications are written on the P2ROM™ by the equipment manufacturer and then provided to the users of the relevant equipment. Although for this purpose the equipment manufacturers need to ensure that unauthorized use, such as the duplication of data by users, is prevented and it is also essential to prevent the leakage of such data especially when it contains personal information. For this reason the loading of security functions is strongly recommended for the P2ROM™, which is used as a storage media for such data.

By loading a data encryption function to the P2ROM™ it is possible to guarantee security for the data stored on the P2ROM™. Encryption of data with the P2ROM™ more specifically, involves the encryption of information over one or both of the two communication paths of the P2ROM™. One of the communication paths encrypted is the command entry path, while the other is the data output path.

A block diagram depicting an encryption function mounted on the P2ROM™ with embedded gate arrays is shown in **Figure 3**.

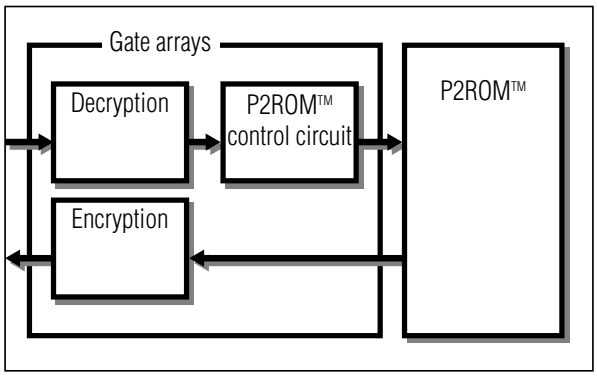

Fig. 3 Block diagram of the P2ROM™ with embedded gate arrays

When a command entry path is encrypted the P2ROM™ becomes a recipient of encrypted data. For this reason the P2ROM™ incorporates a function for decrypting the encrypted command entry by using a decryption key. For example the control circuit of the P2ROM™ follows the decrypted commands and inputs the sequence of read commands to the P2ROM™. Further, the P2ROM™ becomes the sender of encrypted data when the data output path is encrypted, as it would need to incorporate a data encryption function that uses an encryption key.

The keys used in encryptions and decryptions are stored in nonvolatile memory. Difficulties relating to learning about the encryption key or the decryption key, as well as difficulties relating to the tampering of such keys are critical factors for measuring the strength of an encryption method. It is possible to rewrite data on nonvolatile memory, such as Flash ROM, however, there is a risk that the location where the key is stored will be found and the key will be tampered with. Whereas with the P2ROM™, which has a characteristic that does not allow it to rewrite any data, there is no risk of a key being tampered with and therefore, it is possible to achieve a more robust encryption than the type obtained with Flash ROM.

Next we consider the processing time required for the encryption. Once the data output path of the P2ROM™ is firmly encrypted it is possible to guarantee the security of the data stored in the P2ROM™. Since the encryption processing time for the data output path has a direct impact on the reading time of the data, the application of a strong encryption algorithm to this path will deteriorate the performance of the P2ROM™. For this reason, combining the encryption of an input command with the encryption of output data would be an efficient way to use the P2ROM™. This means that by enhancing the encryption on the input command path, for which access is relatively less frequented in comparison with output data path, encryption of the output data path can be made simple and at a high-speed, while still retaining a strong encryption for the P2ROM™.

Testing Method for Encryption Function of P2ROM™

Security of the data stored in the P2ROM™ is guaranteed with the loading of an encryption function in the gate array section, which means the shipping inspection of the chip require special consideration.

A test pattern and configuration diagram of the P2ROM™ is shown in **Figure 4**. In order to perform the shipping inspection for the P2ROM™ loaded with an encryption function, it is necessary to enter an encrypted command and decrypt the encrypted output data.

Designing P2ROM™ with Embedded Gate Arrays

We have prepared an environment for designing circuits loaded in the gate array regions in the shortest TAT, in order to realize a variety of functions in the gate array regions of individual products. The logical design of gate array circuits can be conducted using logical

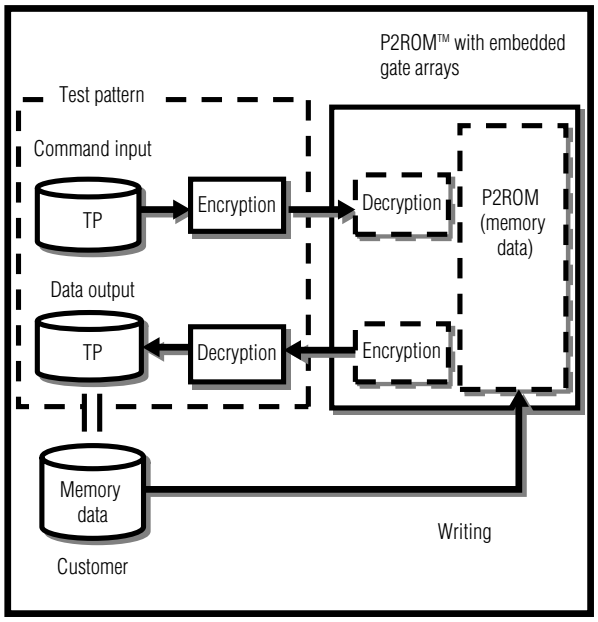

Fig. 4 Test pattern configuration diagram

synthesis, logical SIM, static timing analysis, scan insertions and other such design process flows similar to those of the ASIC design. Also automatic arrangements and automatic wiring are possible for the layout design of gate array regions.

Encryption circuit and other logical circuits are arranged as random logics in the gate array region. Furthermore, since automatic wiring is performed, the wiring layout is generally quite complicated and made across multiple layers. These features improve the tamper resistant characteristics of the encryption.

As mentioned above, embedding gate arrays on the P2ROM™ improves the ease of design for logic circuits, as well as realizes improvements to the encryption intensity.

Prototyping Results

A prototype of a 128M-bit P2ROM™ with embedded gate arrays was created and normal operations were verified. Since the purpose of prototyping was the verification of ASIC design methodologies, the gate array section was loaded with a design of the external clock synchronous-type reading circuit. Measurements were taken with a power supply voltage range of Vcc = 3.0V to 3.6V and an ambient temperature range of Ta = 0 to 80 degrees Celsius, resulting in the verification of an access speed at 23ns and an operating electric current consumption of 18mA. Since these figures are influenced by the control method used, however, these should be considered as reference values only.

Conclusion

Development of the 64M-bit and 128M-bit products has been completed at this time and development of the 256M-bit product has started as a part of the product family's development. We are planning to further extend our development efforts to products with a larger capacity.

Using gate arrays not only makes it possible to customize interface functions, but also to realize a variety of functions. Gate arrays on a large scale are necessary in order to load complex functions, however, the scale varies depending on the application. For our development, we targeted the realization of functions manually designed in the past and aimed for a scale of 20K gates. We will include expansion to the scale of gates in our consideration when developing products in the future and examine the loading of gate arrays on the scale of 40K gates to make it possible to load a variety of commonly used security methods.

Authors

Yoshimasa Sekino: Silicon Solutions Company, LSI Design Div., P2ROM Design Dept.

Hiroyuki Fukuyama: Silicon Solutions Company, LSI Design Div., IP Design Dept.