TOSHIBA REVIEW

2001. VOL.56 NO.7

Special Reports
Information Security

Special Reports
Information Security

*Information Security Fostering Social Progress
IMAI Hideki, D.Eng.

*Overview of and Trends in Information Security Technology
SAISHO Toshiaki KAWAMURA Shin-ichi, D.Eng. ENDOH Naoki

The intensive use of information technology in the political, economic, and cultural areas is essential for the development of society. In any of these areas, security for development has become more important than security for protection. If security is inadequate, new government services, new markets for business, and new entertainment contents cannot be offered.

The fulfillment of Toshiba's role in society is embodied by our superior information security technologies.

*Hierocrypt$_{TM}$ Next-Generation Symmetric Cipher
OHKUMA Kenji, D.Sc. SANO Fumihiko MURATANI Hirofumi, D.Sc.

The symmetric block cipher, which encrypts plain data into an unreadable ciphertext at high speed, is a key component of the information technology society. The Data Encryption Standard (DES), the U.S. federal standard cipher, has been the de facto standard so far. However, the security of DES is no longer adequate because of the rapid improvement of CPU power. The need for 128-bit block ciphers for the next generation has become widely accepted, and the trend of standardization is now active.

To meet this requirement, we have designed a new symmetric block cipher family called Hierocrypt$_{TM}$, which is characterized by the nested substitution permutation network (SPN) structure. The nested SPN structure is very simple, and guarantees high security against differential attacks and linear attacks, which are efficient cryptanalytical methods. Furthermore, the Hierocrypt$_{TM}$ cipher is compact yet it very rapidly encrypts almost all implementations on both software and hardware.

We have proposed the Hierocrypt$_{TM}$ cipher in some standardization projects, and plan to make it widely available for use in many fields such as middleware and smart cards.

*Fast RSA Computation Algorithm and LSI
SHIMBO Atsushi NOZAKI Hanae, D.Sc. KAWAMURA Shin-ichi, D.Eng.

We have developed a fast computation algorithm for the Rivest-Shamir-Adleman (RSA) cryptosystem, which is the de facto standard scheme in public key cryptosystems and digital signatures. This computation algorithm is based on the residue number system, and is a variant of the Montgomery multiplication method. By applying this algorithm, RSA encryption and decryption can be processed in a parallel manner when multiple arithmetic modules are installed in a device. Increasing the number of arithmetic modules results in higher performance.

We have designed an LSI which performs 1,024-bit RSA processing in 2.4 ms by an 80 MHz clock. This LSI is expected to be particularly useful for RSA accelerators installed in servers.

*Identification Technology with Face Image Recognition
FUKUI Kazuhiro YAMAGUCHI Osamu

We have developed a real-time face recognition technology using image sequencing. The face recognition is user-friendly because it can recognize a person without the need for physical contact. It is therefore suitable for use in security systems. To realize practical face recognition, it is necessary to deal with variations in facial expression, face direction, lighting conditions, and other factors. Our method can overcome such variations with image sequencing. This method has been installed in a PC access control system and a facility access control systems.

*Renewable Authentication and Encryption System
TOCHIKUBO Kouya OKADA Koji, D.Eng. ENDOH Naoki

Currently available application systems with authentication and encryption functionality generally use "fixed"encryption and authentication primitives. Alteration or upgrading of these primitives is basically out of their scope. Therefore, considerable time and expense are required to improve the security of the system. Another demerit is that it is difficult to introduce standardized or de facto standard algorithms into the system. Hence, from the viewpoint of application, it is not possible to select or introduce the encryption algorithm that is most appropriate for the value of the information.

We have developed a renewable authentication and encryption system that solves the above problems by allowing primitives to be securely and efficiently altered via the network.

*XML and Digital Signatures
NISHIZAWA Hidekazu SAISHO Toshiaki

Extensible Markup Language (XML) and digital signatures are expected to become important technologies in the electronic commerce and government domains. Toshiba has developed an XML-Signature plug-in with the aim of realizing signing and verification of digital signatures via the Web browser. The signature format is based on the World Wide Web Consortium (W3C) XML-Signature specification. The plug-in implements the common functions of data exchange, and makes form-based document exchange possible without service-dependent application software on the client side.

*Electronic Authentication Based on Commercial Registration System
MAYUZUMI Hiroyuki KANDA Atsushi KOMOTO Takafumi

Electronic commerce has rapidly spread in recent years due to the efficiency and effectiveness of the Internet. In traditional commercial transactions in Japan, a paper-based certificate of a seal issued by a commercial registry office is widely used for authentication of the parties. In electronic commerce, however, a new authentication scheme is required because all transactions should be paperless.

To promote secure electronic commerce, the Ministry of Justice has established a new legal scheme, the Electronic Authentication System based on the Commercial Register, in which an electronic certificate of a digital signature issued by a registry office has equivalent legal validity to the traditional paper-based certificate.

Toshiba has developed a terminal system for the electronic commercial register and delivered it to the Ministry of Justice. Deployment of the system to registry offices throughout Japan has now begun. Toshiba has also developed a software package for corporations that use the certificate for electronic commerce and electronic applications.

*Conditional Access LSI for Broadcast Satellite Service for Mobile Receivers
YURA Koji AKIYAMA Koichiro ISHIKAWA Toshio

Many digital broadcasting services have been realized in recent years. Toshiba is developing a broadcast satellite service (BSS) for mobile receivers. We have developed a conditional access LSI (CALSI) as one LSI of the BSS receiver chip set. CALSI has a new conditional access function based on a new standard conditional access syntax that is suited to BSS. We have confirmed the functionality of the LSI in a test system and verified the effectiveness of the new CA system.

*PKI Construction Services and TARGUSYS$_{TM}$ PKI Card System
NOSE Ken-ichiro ASANOMA Toshiyuki NISHIOKA Mitsuru

Public key infrastructure (PKI) is a security infrastructure using the public key cryptosystem. It is considered an effective way to avoid risks such as unauthorized interception, modification, and fabrication in electronic commerce via the Internet. A certification authority is an important entity which issues a certificate on PKI systems. It is not easy to construct and operate a reliable certification authority.

Toshiba provides PKI construction services for the construction of a certification authority. We have also developed the TARGUSYS$_{TM}$ PKI card system, which provides a highly secure solution by a certificate stored in a smart card.

*Security Consulting Service : Vulnerability Analysis and Intrusion Detection System
YOSHINO Yasuaki HIROSHIMA Kazuhiro KITAORI Shoji

Any information system connected to the Internet could be attacked by crackers located throughout the world. It is therefore necessary to identify holes in security before a system is set up and connected to the Internet. A vulnerability analysis service is helpful for scanning all security holes in the system. Then, when the system is put into operation, an intrusion detection system (IDS) watches for attack signatures and sends an alarm to the administrators.

Our vulnerability analysis service and IDS integration service are parts of the Toshiba security consulting service, which supports the implementation of an enterprise's security policy based on the ISO 17799 international standard.

*Security Features of Toshiba Standard IT System Solutions
YAMADA Asahiko, D.Sc. KOBAYASHI Chieko HARASHIMA Shuji

We are conducting research on security functions for Webtop systems. In Webtop systems, a user must be identified correctly and access to information resources, such as Web contents, Web applications, and databases, is permitted only if the user is authorized to use them.

Toshiba has realized the implementation of a system which performs delegation and single sign-on throughout the information resources. Database systems authenticate the user with authentication information passed by the application, which is stored in the directory server (LDAP server) with confidentiality. This enables us to build a highly secure system in which a user can have access to the information if and only if that user has the right to do so.

*Security Technology for "Mobile Cash"
KATO Takehisa MIYAZAKI Shingo SAISHO Toshiaki

The number of people who access the Internet using cellular phones is increasing rapidly. As a result, several organizations have conducted experiments and introduced services for mobile commerce using cellular phones.

Toshiba has proposed the "Mobile Cash"system in which a cellular phone is used as an electronic wallet, connected to a vending machine with Bluetooth^{TM} wireless technology. This system was prototyped to confirm its security functionality. The elliptic curve digital signature algorithm was used in the system to attain simple and highly secure transactions.

*Security in ETC System
UENO Hideki SUZUKI Katsuyoshi AOKI Megumi

Intelligent transport systems (ITS) are expected to bring about innovation in the social system in the 21st century. As part of the ITS project, the Electronic Toll Collection (ETC) system is now entering the stage of practical utilization. Various security techniques are used in the ETC system in order to protect the privacy of users and secure the proper functioning of the toll collection system.

Toshiba is utilizing its long accumulated know-how in toll collection systems and advanced security technologies in the construction of a wide range of ETC systems. We have now developed a "central system for ETC security" and introduced this system for the first time in Japan.

*Content Protection Technology for DVD-Audio
KATOH Taku, D.Eng. ENDOH Naoki YAMADA Hisashi

DVD is growing into a major storage medium for storing high-quality audiovisual data. Copies of the digital data can be made without difficulty that are exactly the same as the original data. Therefore, the copyright holders of entertainment contents such as movies and music strongly require content protection technology that prevents unauthorized copies from being made when their contents are published.

In order to meet this requirement, Content Protection for Prerecorded Media (CPPM) technology has been adopted as a content protection technology for DVD-Audio. CPPM is suitable for both consumer electronic equipment and PC system implementations.

Techno Notes

*Meeting the Challenge of Medical Solutions

Toshiba Technologies for the New Century

*4. DNA Chip