Paper accepted for presentation at 2009 IEEE Bucharest Power Tech Conference, June 28th - July 2nd, Bucharest, Romania

Protection Relay Systems Employing Unconditionally Secure Authentication Codes

T. Matsumoto, *Member, IEEE,* T. Kobayashi, S. Katayama, K. Fukushima, and K. Sekiguchi, *Member, IEEE*

***Abstract*—The purpose of this study is to produce practical cyber security for protection relay systems using communication channels, such as pilot protection schemes or wide area protection systems. This paper describes a concept and method of effectively applying unconditionally secure authentication codes (A-codes) to such protection relay systems. From the requirements of real-time communication and long-term maintenance of protection relays, we propose a novel scheme based on A-codes having short authenticators (authentication tags) and a feasible number of keys. The efficiency of the scheme is shown by several examples of pilot protection systems and wide area protection systems. The performance and the key management of the proposed algorithm are also discussed.**

***Index Terms*— Power system communication, Pilot protection schemes, Wide area monitoring and control systems, Unconditional Security, Authentication, Authentication codes, Cryptography, Current differential relay**

I. Introduction

Protection relays use communication channels to transmit currents and voltages to each other. A good example of their application is pilot carrier relays, such as directional comparison relays or current-differential relays. Recently, wide area monitoring and protection systems using communication channels and GPS have also been proposed [1]. Possible communication media for protection schemes include point-to-point (optical fiber), microwave, and higher bandwidth transport (SDH, Ethernet). Protection relay schemes with communication systems have seen widespread adoption because of their high efficiency, and there is a growing tendency to adopt Ethernet-based LAN and WAN networks in those communication systems.

In light of this background, the possibility that protection relays will be exposed to growing security threats, including internal attacks, is becoming high. These cyber security issues for protection relays are described in [2]. Many issues in the report are focused on security for maintenance functions of the protection relay, such as passwords, access control, and so on, and security issues involved in protection functions using real-time communication also are mentioned. For real-time communication, IEC 62351 recommends that a Message Authentication Code (MAC) should be generated (as defined in RFC 4634) through the computation of SHA-256 hash function as a general authentication solution for real-time communication data in substations [3]. Another approach that has been proposed is context-based security, using wide area data and decision making with a neural network [4]. To the best of our knowledge, however, there has been little research on practical cyber security based on cryptography against intrusion into communication channels of pilot carrier relays and wide area protection systems.

Considering cyber security requirements, in fact, for most power system operations, authentication of control actions is far more important than "hiding" the data through encryption. It is clear that relay systems need authentication schemes [2], and it should be considered that protection relays must have not only high reliability but also high availability, meaning that continuous service is desired. It is difficult, however, to update the software in these relays during service. With these characteristics, such systems are not always suitable for the so-far proposed authentication methods such as MAC because they employ computational cryptographic primitives commonly used in IT, which cannot provide the assurance of long-term security in view of the inevitable increase in computational power available to opponents or attackers. Moreover, from the requirement of real-time communication for pilot protection relays, the security overhead should be minimized and the algorithm should be simplified in order to verify the operation of the protection relay and quickly detect intrusion.

We propose a novel approach to these issues, which employs unconditionally secure cryptographic primitives based on the information theory initiated by Claude Shannon. In Section II, we present the background and basic idea of our study. Section III deals with case studies in current differential relays and wide area protection systems (WAPS). In Section IV, we discuss the performance of the proposed algorithm. Finally, we comment on the key management scheme in Section V.

II. Application of A-codes To Protection Relay Systems

The idea of perfect secrecy and the use of entropy techniques in cryptography were pioneered by Shannon [5]. Authentication schemes are classified as being

T. Matsumoto and T.Kobayashi are with Yokohama National University, 79-7 Tokiwadai, Hodogaya, Yokohama 240-8501, Japan (email: tsutomu@ynu.ac.jp taiki@mlab.jks.ynu.ac.jp).

S. Katayama, K. Fukushima and K. Sekiguchi are with TOSHIBA Corporation, 1, Toshiba-Cho, Fuchu-shi, Tokyo, 183-8511, Japan (e-mail: shigeki.katayama / kazuto.fukushima / katsuhiko.sekiguchi@toshiba.co.jp).

978-1-4244-2235-7/09/$25.00 ©2009 IEEE

computationally secure or unconditionally secure [6]. A good example of a computationally secure authentication scheme is the conventional MACs. On the other hand, an authentication scheme is said to be unconditionally secure or information-theoretically secure if the security is independent of the computing power or time an opponent can bring to bear; this authentication is referred to as *authentication codes*, or *A-codes*, which are equivalent to the so-called *universal hash families*.

We study A-codes to adopt them for the transmission data in pilot carrier relays. We found that A-codes are suitable for protection relays because of two prominent features:

- Independence of computer power: for several decades after deploying relays, it will not be necessary to update the security software and parameters because of the independence of the computer power of opponents.
- Controllability of opponent's deception probability: A-codes are based on information theory, so that the probability is computable and controllable. In other words, relay engineers can design an appropriate authentication scheme for each protection system.

Suppose the opponent has the ability to insert messages into the channel and/or modify existing messages. When the opponent places a new message into the channel, this is called impersonation. When the opponent sees a message and changes it to another message, this is called substitution. Once the transmitter/receiver have chosen the authentication strategy, it is possible to determine a probability P_{di} (for $i = 0$, 1), which is the probability that the opponent can deceive the transmitter/receiver by impersonation and substitution, respectively. It is not difficult to show that $P_{d0} \geq 1/m$ and $P_{d1} \geq 1/m$ [9], where m is the number of possible authenticators, each of which is a bit string determined based on the data to be protected (source state) and the key. An authenticator is also called an authentication tag.

The firstly published paper on A-codes was by Gilbert, Williams and Slone [7]. Although A-codes can be theoretically very secure and their general theory has been continuously developed by many cryptologists, including Simmons [6], Wegman and Carter [8], and Stinson [9], the concept is not so widely known to outside cryptographic research community and they have been rarely used in practical applications. The main reason may be that, to generate an authentication tag, part of the key is consumed, which implies that a huge number of keys is required when many packets are transmitted. Additionally, appropriate use of A-codes requires rigorous management for sharing and maintaining keys.

In order to achieve both negligible deception probability and reasonable key size, as well as a dependable implementation, here we introduce a novel A-code scheme. To illustrate our idea, we give a concrete example whose principle is outlined in Equation (1) and Fig. 1. (In Equation (1), the multiplication and addition of each component of a vector and a matrix is just the logical AND operation and Exclusive OR operation, respectively.)

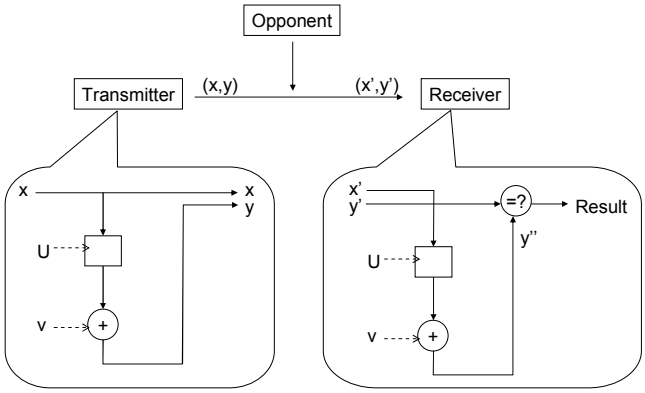

Fig. 1 A-codes for protection relay scheme.

At the transmitter, an authentication tag is generated for each source state (i.e., sampled voltages and currents, or phasor voltages and currents), using a set of keys (U, v), at a certain timing (e.g., analogue data sampling timing or phasor calculation timing). The transmission data consists of a source state x and its authentication tag y, which are periodically sent through the communication channel.

At the receiver, the received source state x' and authentication tag y' of the transmission data are authenticated using a key identical to the key located at the transmitter.

$$y = x\,U + v \tag{1}$$

where,

- x: a-bit vector representing a source state
- U: binary matrix with a rows and b columns
- v: b-bit vector
- y: b-bit vector representing an authentication tag for x
- +: bit-wise Exclusive-OR operation.

To make an authentication tag, the calculation of (1) is necessary. The computation has relatively low complexity and is readily performed by the protection relays. At each time step, a fresh v is required, but U can remain unchanged. The scheme is quite simple, but it achieves deception probabilities $P_{d0} = P_{d1} = 1/2^b$.

The set of keys, each of which is used once, is preinstalled in each relay (transmitter and receiver). They can be distributed and installed by maintenance personnel, similar to the way that settings are currently managed in a rigorous manner, when relays are deployed and start service.

III. Case Studies

A current differential system is a popular pilot protection scheme. The current differential scheme compares the magnitudes and phases of the currents from all terminals. Although current differential relays have good characteristics, the relay scheme requires low-latency and highly deterministic communication channels and is dependent upon the reliability of the communications. We consider transmission data with authentication tags of the current-differential relay, and we show the effect of the proposed scheme.

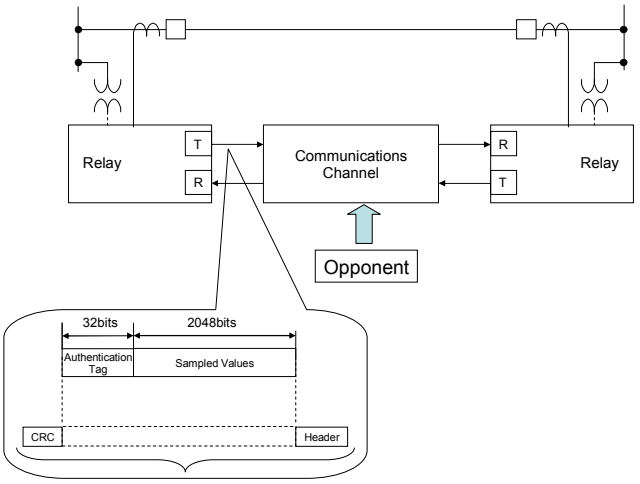

Fig. 2 Current-differential relay scheme and transmission data.

Fig. 2 shows the current-differential relay scheme and the transmission data with an authentication tag appended to the source state. The parameters in the example are as follows:

Sampling rate:	4800 samples per second (System frequency 50 Hz)
Transmission rate:	600 Hz
Frame data length:	2048 bit
Operation period:	20 years
Authentication tag length:	32 bit.

The deception probabilities are given by:

$$P_{d0} = P_{d1} = 1/2^{32} = 2.33 \times 10^{-10} < 10^{-9} \quad (2)$$

and

$$\begin{aligned} S &= 32 \text{ bit} \times (2048 + \text{the number of transmissions during 20 years}) \\ &= 4 \text{ Byte} \times (2048 + 600 \times 60 \times 60 \times 24 \times 365 \times 20) \\ &= 4 \times 3.8 \times 10^{11} \\ &= 1.5 \text{ TByte} \end{aligned} \quad (3)$$

where S is the necessary key memory size.

The relatively large key memory size of 1.5 TB may be not a critical problem for protection relays in the future, because widely available flash memory chips can record up to 32 GB today, and Moor's law hints that it will be possible to install 1 TB flash memories for storing keys in each relay in years to come. Alternatively, by optimizing the parameters in (1), it may be possible to reduce the memory size to several tens of MB, which is more practical and reasonable.

The deception probabilities of 2.33×10^{-10} are so small that the proposed scheme can provide a very secure system. For example, the opponent's deception probabilities are rather less than the misdetection rate of CRC-CCITT (16-bit CRC), which is known to be $2^{-16} = 1.53 \times 10^{-5}$ for random noise. CRC-CCITT is one of the most widely used error detection codes employed in not only pilot carrier relay communications but in general power system communications. It suggests that a 1.5 TByte key memory size can provide relay systems with enough reliability and security. Alternatively, for realizing the conventional reliability with a misdetection rate of 1.53×10^{-5}, we need a memory size of about 750 GByte, which is deduced by the formula (3). For the other example, considering the 32-bit CRC used on Ethernet LANs, its misdetection rate of $2^{-32} = 2.33 \times 10^{-10}$ is equal to the probability of the opponent's deception , which is obtained by using a memory size of 1.5 TByte.

Fig. 3 shows the opponent's deception probabilities with necessary key memory size at each transmission rate, where we assume that the operation period is 20 years, and the transmission rate means the number of transmission frames per second. It suggests that the transmission rate should be restricted if the key memory size is required to be smaller. For example, when current differential relays transmit sampled instantaneous values of currents at 600 Hz transmission rate, the required key size is 1.5 TByte. On the other hand, when Phasor Measurement Units (PMU) of Wide Area Protection Systems (WAPS) transmit phasor values of currents at 60 Hz transmission rate under the same conditions as in the instantaneous values case, the key size is 150 GByte, which is far smaller than the key size in the instantaneous values case. Additionally, it is important that the opponent's deception probability is independent of the frame length.

As shown above, when an adequate number of keys are prepared, A-codes can achieve long-term maintenance-free security. The required key storage in the relays depends on the transmission rate, the system configuration, the operation period, and the reliability to be achieved. Thus, if these parameters are variable, such as in communications commonly used in IT, the required key storage cannot be estimated. Fortunately, in protection systems, we can define these parameters so clearly at our system engineering stage that the needed key storage can be estimated definitely.

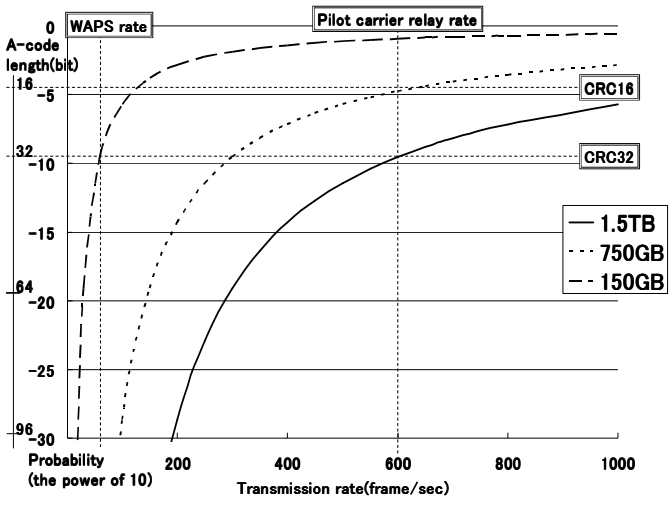

Fig.3 Changes of the opponent's deception probabilities.

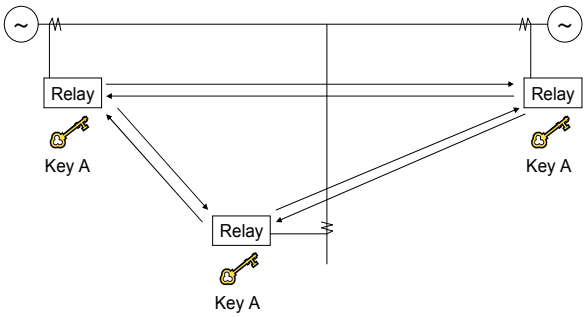

Fig. 4 (a) Multi-terminal current differential relay system

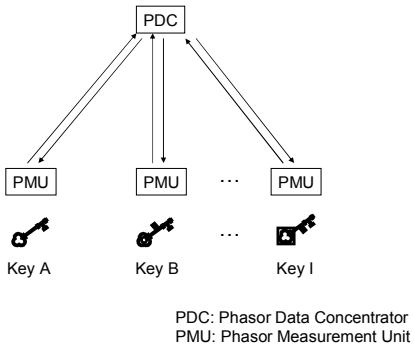

Fig. 4 (b) Wide area protection system.

In this study, we have also investigated other examples, including multi-terminal current differential relays and wide area protection systems. Although the performance and efficiency of these other protection systems are the same as those of the above two-terminal current differential relays, the methods of dealing with the keys differ.

Fig. 4(a) shows a configuration example of a multi-terminal current differential protection relay system that extends the two-terminal system shown in Fig. 2. In this case, each relay installed in each substation can share the same key (Key A) and use it to calculate authentication tags of A-code because the system configuration rarely changes after installation. Fig. 4(b) illustrates an example of a wide area protection system which consists of PMUs, a phasor data concentrator (PDC), and communication channels between the PMUs and PDC. In this system, it is difficult for the PMUs to share the same key because each PMU might be plugged into the system after the system operation is initially started, in order to adaptively deal with various requirements for wide area protection and control. Thus, each PMU should have its own key (Key A, Key B, ... Key I), and calculate authentication tags of A-code with the key. When a PMU is plugged into the system, the same key as that of the PMU will be installed in the PDC.

For control systems such as Supervisory Control and Data Acquisition (SCADA) and Substation Automation System (SAS), the necessary key memory size can be much smaller than protection systems because the number of frames including control commands and event information is fewer and the frames are not transmitted periodically, unlike protection systems. Thus, we assume that the average transmission rate is one frame per second, considering worst-case conditions, including periodical metering. The parameters in the example control systems are as follows:

Operation cycle:	1 operation per second
Frame data length:	2048 bit
Operation period:	20 years
Authentication tag length:	32 bit.

The intrusion probabilities are given by:

$$P_{d0} = P_{d1} = 1/2^{32} = 2.33 \times 10^{-10} < 10^{-9} \tag{4}$$

and

$$\begin{aligned} S &= 32 \text{ bit} \times (2048 + \\ &\qquad \text{the number of operations during 20 years}) \\ &= 4 \text{ Byte} \times (2048 + 60 \times 60 \times 24 \times 365 \times 20) \\ &= 4 \times 0.6 \times 10^9 \\ &= 2.4 \text{ GByte} \end{aligned} \tag{5}$$

where S is the necessary key memory size.

In all of the above cases, it is necessary for both the transmitter and receiver to completely synchronize their keys for calculating A-codes. There are some ways to achieve this synchronization. For example, both the transmitter and receiver are provided, in advance, with unique sequence numbers to keys. The transmitter sends the frame including the sequence number of the key with which the transmitter calculates authentication tags of A-code. The receiver also calculates authentication tags of A-code with the key which is indicated by the sequence number in the received frame.

In previous studies regarding cryptographic technologies for real-time power communications [10], it was important to discuss the properties of communication channels, the protocol used over the channel, and the relaying application, for example, fiber or power line, owned media or leased line, Distributed Network Protocol (DNP) or others, current differential or direction comparison, sufficiently secure line or not sufficiently secure, and so on. Our proposed algorithm might free us from these discussions because it is so simple, has a small overhead, and is mostly independent of the communication environment.

IV. Performance Results

In order to verify that our proposed algorithm introduced in formula (1) is suitable for real-time protection communications, we implemented it as C-language software and measured its execution time on both a PC and a relay. The test environments and the measured execution time are summarized in Table I. Although the execution times were independent of source data x, the execution time on the relay can vary a great deal because of the CPU cache hit/un-hit.

Under the test environments, a 40-bit authentication tag was generated from 2048-bit source data on each type of hardware. The execution times for generation were measured and

TABLE I
TEST ENVIRONMENTS AND EXECUTION TIMES

	PC	Relay
CPU	Pentium D 3.2 GHz	MIPS 32 bit architecture CPU 333 MHz (Data and instruction cache size are 32 KB, respectively)
RAM	3.49 GB	64 MB
OS	Windows XP Professional in Safe Mode	ITRON (Real-time Operating system)
Compiler	Microsoft Visual C++ 6.0	Standard compiler provided by CPU manufacture
Execution Time (microsecond)	2.67–2.73	79–139

compared. We found that the execution time on the PC test set was very short, but that on the relay test set was slightly long for current protection differential relays. Considering relaying applications and communication processing, the desirable execution time for authentication tag generation is less than 10 microseconds.

To cope well with the challenge, we have been studying several implementation methods. One of the methods, which has already been adopted in the above testing, is pre-calculating which involves multiplying a binary matrix U by all patterns of s-bit blocks (i.e., 2^s patterns), storing the results in advance as a pre-calculating table, and searching the table according to the source data x. This method can compress the execution time to 1/s compared to multiplying each source data x by the binary matrix U in real time, although it needs some memory space for the pre-calculating table. Optimizing the parameter s remains an issue. One of the other methods is to use a long word length processor. For example, 64 bit processors for embedded applications can shorten the execution time. When the proposed algorithm based on a 32 bit authentication tags is implemented with 64 bit instructions, we have estimated that the execution time can be about 25 % shorter than with 32 bit instructions.

These results above show that the proposed algorithm has the possibility of achieving sufficiently short execution time for real-time protection communication with some increase of the CPU cache size and improved implementation. It is important to remember that the clock speed of CPU for embedded applications, such as protection relays, might be restricted by thermal issues, which has an impact on the cost and reliability of the relays. Thus, the proposed algorithm is suitable for relay systems because it does not need a high speed processor, as shown in the above discussion. On the other hand, computational cryptographic schemes commonly used in IT generally consume relatively large amount of CPU power. For example, when we measured the execution time of SHA-256 implemented as C-language software on the PC in Table 1, the execution time was more than several hundred microseconds, indicating that HMAC with SHA-256 software implementation needs a lot of CPU power to be adopted in relay systems, which will cause thermal problems.

V. KEY MANAGEMENT

In this section, we discuss the key management for the proposed system. If an opponent steals the key, it is easy for the opponent to deceive the transmitter/receiver by impersonation and substitution. Thus, the proposed system needs secure key management, including key generation, key distribution, and key setting. Fig. 5 illustrates a typical key management scheme for a current-differential relay system.

For the key generation, the key for calculating authentication tags should be generated with a pure random number generator in a maintenance room in a control station. We cannot adopt pseudorandom number generators for this purpose because the very basis of unconditional security of A-codes comes from the randomness but not from pseudo randomness. For the key distribution, the generated key is copied and delivered to both terminals (substation A and B) mainly by car. For the key setting, the key is installed into the flash memory ("F-ROM" in Fig. 5) of each relay, and the relays start real-time communication with the A-codes. Most modern numerical relays have a communication port ("ETH" in Fig. 5) to connect maintenance tools from the maintenance room via non-real time communication channels.

Even if the real-time communication channel could be made completely secure by employing the A-code, Fig. 5 shows that there are many possible threats. For example, one is the method used to carry the key to each substation. An opponent might attack the car and steal the key. Another is that opponents might hack the maintenance communication and take over the relay. Moreover, there have been many unpublished cases where control and diagnostic systems have been impacted by cyber incidents in electrical power systems, including transmission substations. The traditional concerns of electric utilities about the security of their substation assets have centered on protecting the substation from physical threats, both natural and human threats [11]. The literature introduces five threats. Considering these threats, the keys should be encrypted before being carried to the substations. They might be decrypted and installed into the F-ROM at a HMI (Human Machine Interface), or installed into the F-ROM without decryption. In the latter case, they would remain secure even if the F-ROM data were stolen, but the relays will decrypt the keys before authentication tags are calculated. To avoid intrusion from the maintenance communication, it is effective to protect the communication channel with A-codes also. Alternatively, a common computational security based cryptographic methods used in IT system, such as AES or SHA, could be used because this communication is not used for protection directly, and therefore, it is usually easier to maintain and update than real-time communication.

To develop practical and systematic way of key management for cryptographic application in power systems

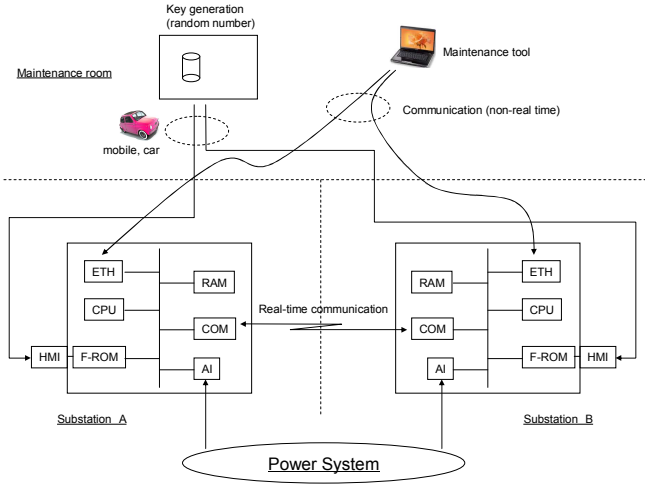

Fig. 5 Key Management Scheme.

communication may require further discussions.

VI. Conclusions

One well-known realization of unconditional security is the one-time pad, which provides perfect secrecy but has been limited in commercial applications because of key management problems and key length. Similarly, there have been few real-world applications for A-codes, but we show that A-codes are suitable for protection relay systems and other power applications.

The proposed authentication scheme can be managed by protection relay engineers or power communication engineers, because the opponent's deception probabilities can be calculated. Moreover, this approach involves no risk in terms of advancing computing power and aging cryptography algorithms, and also benefits from ease of authentication tag generation and verification.

The proposed method is suitable for adoption not only in pilot carrier relays and in wide area protection systems, but also in general power systems, such as SCADA or substation automation which use real-time communication and in which software or firmware updating is difficult and there is a need for deterministic responses to events.

VII. Acknowledgments

The authors gratefully acknowledge the contributions of Dr. Junji Shikata, Takehiro Furue, Masayoshi Shigeta and Shota Nii for their comments and suggestions. Thanks also to Atsushi Kasai and Sinji. Iinuma for their generous supports.

VIII. References

[1] D. Novosel, V. Madani, B. Bhargava, V. Khoi and J. Cole, "Dawn of the Grid Synchronization", IEEE Power & Energy Magazine, January/February, 2008, 49-60.

[2] "Cyber Security Issues for Protective Relays" PSRC WG-Report C1, Jan. 2007.

[3] IEC 62351, "Power systems management and associated information exchange - Data and communication security".

[4] Su Sheng, W. L. Chan, K. K. Li, D. Xianzhong and Z. Xiangjun, "Context Information-Based Cyber Security Defense of Protection System", IEEE Trans. Power Del. Vol. 22, No. 3, JULY 2007.

[5] C. E. Shannon, "Communication theory of secrecy systems", Bell Systems Technical Journal, 28, 1949, 656-715.

[6] G. J. Simmons, "A survey of information authentication", Proceedings of the IEEE, 76, 1988, 603-620.

[7] E. N. Gilbert, F. J. MacWilliams and N. J. A. Sloane, "Codes Which Detect Deception", Bell Systems Technical Journal, 53, 1974, 405-424.

[8] M. N. Wegman and J. L. Carter, "New hash functions and their use in authentication and set equality", Journal of Computer and Systems Sciences 22, 1981.

[9] D.R. Stinson, "Universal hashing and authentication codes", CRYPTO, 1991.

[10] A. Risely, J. Robert and P. LaDow, "Electric security of real-time protection and SCADA communications", WPDAC, Apr. 2003.

[11] J. D. McDonald, ed. Electric Power Substations Engineering, Second Edition, CRC Press, 2007

IX. Biographies

Tsutomu Matsumoto is a professor at the Division of Social Environment and Informatics, Graduate School of Environment and Information Sciences, Yokohama National University. He received his Dr. Eng. Degree from the University of Tokyo in 1986 and since then he has been based at Yokohama National University and studying Information and Physical Security. He is an associate member of the Science Council of Japan, a research advisor of the Research Center for Information Security at the National Institute of Advanced Industrial Science and Technology and a core member of the Cryptography Research and Evaluation Committees for governmental use of cryptography. He is a director of IACR - International Association for Cryptologic Research as well as a member of IEEE, IEICE, and IPSJ.

Taiki Kobayashi received his B.E. degree in electrical and computer engineering from Yokohama National University in 2009. He is currently studying cryptology and information security at the Graduate School of Environment and Information Sciences, Yokohama National University.

Shigeki Katayama received his BS degree and MS degree in applied mathematics and physics engineering from Kyoto University in 1997 and 1999, respectively. And he joined Toshiba Corporation in 1999. He is now engaged principally in the development of protection and control systems. He is the leader of security related R&D issues in his section.

Kazuto Fukushima received his BS degrees in electrical engineering from Osaka Sangyo University, Osaka, Japan. He joined Toshiba in 1993, and is working as a protection and control system engineer in Toshiba Corporation. He is a member of IEEJ.

Katsuhiko Sekiguchi received the B.S. and M.S. degree in communication engineering from Tohoku University, Sendai, Japan, in 1979 and 1981 respectively. He joined Toshiba Corporation in the same year and has been engaged in the development of protection relays and network computing applications for power system protection & monitoring. He is a member of IEEJ, IEEE and CIGRE.