ABSTRACT

An important problem in cryptography is to satisfy secure data communication over an insecure channel. Usually, computing technologies such as E-mail, on-line Banking, ATMs, Mobile Applications, IoT, Big data, Cloud Network, VANET, and MANET require secure and efficient cryptographic solutions. Now-a-days, the trade-off between security and efficiency is the most significant issue for designing a handy cryptographic solution. Generally, the cryptographic solution should be suitable to implement in variety of platforms like IoT environment, cloud network, metropolitan area network, big data environment, and smart city. In addition, it should satisfy reasonable efficiency with satisfactory security margin. Under symmetric key cryptography, certain tools are used to keep secure data communication. Among these tools, one of the important tool is cryptographic compression function.

The Cryptographic Compression Function (CCF) is used as a component of cryptographic hash (CH). The cryptographic hash is defined as to proceed data from an arbitrary domain to a fixed domain. Applications of the CH are enormous such as message verification, password verification, and pseudo-random generation. Generally, the CCF is built by scratch or block-cipher. Interestingly, the block-cipher based CCF is more apposite than the scratch based CCF because of direct hardware implementation of block-cipher. Depending on the output size of block-cipher, there are two more groups such as single block-length (SBL) and double block-length (DBL). However, the SBL is not appropriate because of the birthday-bound attack. On the contrary, the DBL has three more sub-groups depending on the key size such as (n, n), (n, 2n) block-cipher based CCF, and (n, k) light-weight cipher based CCF. Under the (n, n) CCF, there are certain familiar schemes such as MDC-2, MDC-4, MJH, and Bart-12. The most of the schemes of (n, n) based CCF cannot support variable size of message encryption. In addition, padding mechanism is mandatory for small and flexible size of message. These familiar schemes have less collision security bound and less efficiency-rate. Oppositely, the existing schemes of (n, 2n) block-cipher CCF are classified under two classes which are based on rigorous security bound and efficiency. Usually, the efficiency-rate (r) is defined as r=|m|/n*(#E) where |m| means length of message, n directs block-length, and #E indicates number of calling block-cipher. The schemes of Weimar-DM, Hirose-DM, Tandem-DM, and Abreast-DM are members of the rigorous security bound group. These schemes are secure under the ideal cipher model (ICM). However, the security assumption of the ICM

is very rigid. Hence, adversary model is weak under this security proof model. In addition, the ICM is close to the ideal world rather than the real world. On the contrary, Nandi and ISA-09 belongs to the efficiency class. These schemes need three calls of block-cipher. In addition, key scheduling is KS=3. Moreover, the operating mode is serial. From the above discussions of CCF, the desired targets are:

- Upper security bound, Higher efficiency-rate, Less call of block-ciphers, Less key scheduling, and Better security proof model (close to the real world).

Next, we use Cryptographic Compression Function as a building tool in the domain of Authenticated Encryption (AE). Generally, AE is a procedure that satisfies both data privacy and authenticity. The AE has many applications in the field of secure data communication such as e-banking, mobile banking, IoT, big data, and cloud network. Generally, AE consists of two modules such as Encryption and Decryption. Input of encryption module is respectively message, key, nonce, and optional associated data (AD). Usually, nonce is defined as the counter or unique number. On the contrary, cipher-text and authentication tag are output of encryption module. Generally, this tag is noted as T (n-bit) that is used for message authentication. Moreover, cipher-text, key, authentication tag, and optional AD are the input of decryption module. In addition, if authentication tag is matched for the supplied cipher-text then output of decryption module is plain-text else error. According P. Rogaway, there is another concept of IV. We define probabilistic-IV-based AE or IV-based AE in short as an authenticated encryption algorithm that has a random IV without associated data whose security goal is indistinguishability with random bits with respect to an adaptive-chosen-plaintext-and-known-IV attack, unlike the common security goal of AE with nonce and associated data, which is indistinguishability with an adaptive-chosen-plaintext-and-IV attack. Under these circumstances, we classified two groups of probabilistic-IV-based AE and nonce respect (including AD) AE. Under the nonce, AD based AE schemes, there are two more subgroups in respect of security notions such as nonce respect and nonce reuse. Usually, nonce respect means the value of each nonce is unique like counter. Oppositely, if nonce value is repeated, then it is called nonce reuse. In the domain of nonce, AD based AE, the most important argument is whether the AE is secure and authentic under the nonce reuse. Interestingly, E. Fleischmann et al. claimed that nonce reuse is acceptable in the aspect of security notions of AE through the scheme of McOE. Following that, several schemes have been proposed like APE, PoE, TC, COPA, and ElmE-D. However, Hoang et al. proved that usage of nonce reuse is not secure and proper in the aspect of security notions of online AE. Hence, a door is re-opened for security notions of nonce respect in AE.

Usually, nonce and AD based AE satisfies rigorous security bound. However, overhead costs are increased because of strong security model. Under the recent trends of information technology, the IoT, big data, and cloud network are emerging applications. Interestingly, the main challenges of IoT-end devices, big-data end devices and cloud network low level devices are to keep a certain level of security margin with low cost. Thus, the AE should satisfy the properties of low cost and resources also including reasonable security bound. We actually try to address that using secure cryptographic compression function, it is possible to build secure and efficient authenticated encryption. In addition, we have some proposals of authentication mode under the authenticated encryption scheme those have opportunity to provide higher authenticity security margin.

- Propose certain ideas of AE that are based on cryptographic compression function, Better efficiency, Application based AE (light, heavy scheme, and secure scheme), Parallel operating mode, Less call of block-cipher function.

In addition, Small Domain Message Encryption (SDE) is another application of CCF. It is one of the most prominent branch of message encryption where message domain should be small. Usually, it is defined as to encrypt short message where plain-text and cipher-text are equal in length including similar format. The SDE is widely implementable under personal identification, and ATMs. There are certain familiar schemes those are based on card shuffling algorithm where block-cipher is used as primitive. The schemes of Swap-or-not shuffle, Mix and Cut, Thorp shuffle, and SRS are based on block-cipher (e. g. AES), where the number of calling block-ciphers or functions are high. Hence, these schemes are not efficient for encryption under the resource constrained devices and IoT-end devices. From the above discussions of TDE, the desired targets are:

- Supports small encryption function, Satisfy reasonable security margin

Keywords. Cryptographic Compression Function, Authenticated Encryption, Small Domain Encryption, Collision Resistance, Efficiency-rate