通信情報保護學會誌
第5卷 第2號, 1995. 6

ISO/IEC JTC1/SC27의 국제표준소개 (8) : ISO/IEC IS 10118-1 정보기술 - 보안기술 - 해쉬함수, 제 1 부 : 개론

(Information technology - Security techniques - Hash - function - Part 1 : General)

이 필 중*

요 약

지난 세번에 걸쳐 소개하던 실체인증기법을 중단하고 이번호 부터는 해쉬함수 국제표준을 소개한다. 국내에서도 표준화 노력이 진행되고 있는 해쉬함수는 임의의 길이의 비트스트링을 정해진 길이의 출력인 해쉬코드로 변환시키는 함수로서 디지탈서명, 인증, 키 분배등의 많은 적용사례를 갖고 있다. 해쉬함수의 표준화 과제는 1984년 디지탈서명 국제표준화 과제중 한 part로 시작했다가 1989년 독립된 과제가 되었다. 그 당시에는 2개의 part(Part 1 : General, Part 2 : Hash-functions using an n-bit block cipher algorithm)로 시작되었다가 나중에 2개의 part (Part 3 : Dedicated hash-functions, Part 4 : Hash-functions using modular arithmetic)가 추가되었다.

이 과제는 1991년 CD(Committee Draft), 1992년 DIS(Draft for International Standard)가 되었고, 1993년에 IS(International Standard)가 되었고 1998년 1차 검토가 있을 예정이다.

1. 범 위 〔Scope〕

국제표준 ISO/IEC 10118은 해쉬함수를 상술하며 따라서 인증, 무결성과 부인봉쇄 서비스를 규정하는데 적용될 수 있다. ISO/IEC 10118의 모든 부분에서 해쉬함수의 입력스트링은 데이터스트링이라 부르고 출력스트링은 해쉬코드라 부른다. 〔International Standard ISO/IEC 10118 specifies hash-functions and is therefore applicable to the provision of authentication, integrity and non-repudiation services. For the purposes of all parts of ISO/IEC 10118, the input string of a hash-function is called a data string and the output string is called a hash-code.〕

㈜ 비밀키를 사용하여 메세지 인증을 보증하기 위해 메시지인증코드(MAC)를 계산하는 경우와는 달리 해쉬코드를 생성하는 경우는 비밀키를 사용하지 않는다. MAC의 계산을 위

* 종신회원, 포항공과대학교 전자전기공학과

해서 ISO/IEC 9797을 참조하라. [NOTE - In contrast to the calculation of a Message Authentication Code (MAC), the goal of which is to ensure authentication of a message employing a secret key, the generation of a hash-code does not involve a secret key. For the calculation of the MAC the user is referred to ISO/IEC 9797.]

이 ISO/IEC 10118의 제 1부에서는 이 국제 표준의 모든 다른 부분에서 공통적으로 사용되는 정의, 기호, 약어와 요구조건을 기술한다. [This part of ISO/IEC 10118 contains definitions, symbols, abbreviations and requirements which are common to all the other parts of this International Standard.]

2. 용어 정의 [Definitions]

ISO/IEC 10118의 모든 부분에서 다음의 용어 정의가 적용된다. [For the purposes of all parts of ISO/IEC 10118, the following definitions apply :]

2.1 충돌 저항형 해쉬함수[collision-resistant hash-function] : 다음의 특징을 갖는 해쉬함수

- 같은 출력을 가지는 서로 다른 두 개의 입력을 찾는 것은 계산상 실행불가능하다. [A Hash-function satisfying the following property: - it is computationally infeasible to find any two distinct inputs which map to the same output.]

㈜ 계산상 실행 가능성의 여부는 사용자의 특별한 보안 요구와 환경에 영향을 받는다. [NOTE - Computational feasibility depends on the user's specific security requirements and environment.]

2.2 데이터스트링(데이터)[data string (data)] : 해쉬함수의 입력인 비트스트링. [The string of bits which is the input to a hash-function.]

2.3 해쉬코드[hash-code] : 해쉬함수의 출력인 비트스트링. [The string of bits which is the output of a hash-function.]

㈜ 관련 문헌은 해쉬코드와 같거나 비슷한 의미를 갖는 다양한 용어를 사용하고 있다. 변경검출코드, 조작검출코드, 요약, 해쉬 결과, 해쉬값과 흔적이 그 예이다. [NOTE - The literature of the subject contains a variety of terms which have the same or similar meanings hash-code, Modification Detection Code, Manipulation Detection Code, digest, hash-result, hash-value and imprint are some examples.]

2.4 해쉬함수[hash-function] : 비트스트링을 다음의 두 가지 성질을 만족하는 고정된 길이의 비트스트링으로 대응시키는 함수

- 주어진 출력에 대하여 이 출력을 생성하는 입력을 찾아내는 것은 계산상 실행불가능하다.
- 주어진 입력에 대하여 같은 출력을 생성하는 또 다른 입력을 찾아내는 것이 계산상 실행불가능하다. [A function which maps strings of bits to fixed-length strings of bits, satisfying the following two properties: - it is computationally

infeasible to find for a given output an input which maps to this output; - it is computationally infeasible to find for a given input a second input which maps to the same output.〕

㈜1 관련 문헌은 해쉬함수와 같거나 비슷한 의미를 갖는 다양한 용어를 사용하고 있다. 압축 부호화와 축약 함수가 그 예이다. 〔NOTE 1 - The literature of the subject contains a variety of terms which have the same or similar meaning as hash-function. Compressed encoding and condensing function are some examples.〕

㈜2 계산상 실행가능성의 여부는 사용자의 특별한 보안 요구와 환경에 영향을 받는다. 〔NOTE2 - Computational feasibility depends on the user's specific security requirements and environment.〕

2.5 초기값〔initializing value〕 : 해쉬함수의 시작점을 정의하는데 사용된 값 〔A value used in defining the starting point of a hash-function.〕

2.6 덧붙이기〔padding〕 : 데이터스트링에 추가적인 비트를 붙이는 것 〔Appending extra bits to a data string.〕

3. 기호와 약어〔Symbols and abbreviations〕

ISO/IEC 10118의 모든 부분에서 다음의 기호와 약어가 사용된다. 〔Throughout all parts of ISO/IEC 10118, the following symbols and abbrebiations are used:〕

D 데이터〔Data〕
H 해쉬코드〔Hash-code〕
IV 초기값〔Initializing value〕
Lx 비트스트링 X의 비트 길이〔Length (in bits) of string of bits X〕
X ‖ Y 비트스트링 X와 Y의 연결〔Concatenation of strings of bits X and Y〕
X⊕Y 비트스트링 X와 Y의 배타적 논리합〔Exclusive-or of strings of bits X and Y〕

모든 비트스트링은 첫 비트가 가장 왼쪽에 쓰여진다. 〔All strings of bits are written with the first bit in the leftmost position.〕

4. 요구 사항〔Requirements〕

해쉬함수를 이용하기 위해서, 참여하는 실체들은 각각의 실체의 환경에서 표현방식이 다를지라도 정확하게 같은 데이터를 사용해야한다. 이때문에 하나 이상의 실체가 해쉬함수를 적용하기 전에 데이터를 합의된 표현방식으로 전환해야 될 수도 있다. 〔The use of a hash-function requires that the parties involved shall operate upon precisely the same data, even though the representation may be different in each entity's environment. This may require one or more of the entities to convert the data into an agreed representation prior to applying a hash-function.〕

ISO/IEC 10118에 상술된 어떤 해쉬함수는 하나 혹은 그 이상의 초기값을 사용한다. 이 경우에 해쉬코드를 생성하는 실체와 그것을 확인하는 실체가 같은 초기값을 사용하는 것을 보증하기 위해 필요한 규정을 만들어야 한다. 이러한 규정의 예는 부록 A에 제시되어 있다. 〔Some of the

hash-functions specified in ISO/IEC 10118 use one (or more) initializing value(s). In this case, provisions shall be made in order to ensure that the entity which produces the hash-code and the one which checks it shall use the same initializing value(s). Examples of such provisions are presented in annex A.〕

ISO/IEC 10118에 상술된 어떤 해쉬함수에서는 데이터스트링을 요구되는 길이로 만들기 위해 덧붙이기가 필요하다. 덧붙이기 방법은 덧붙이기가 필요한 ISO/IEC 10118의 각 부분에 상술될 수 있다. 이러한 방법의 예는 부록 B에 제시되어 있다. 〔Some of the hash-functions specified in ISO/IEC 10118 require padding, so that the data string is of the required length. The padding methods may be specified each part of ISO/IEC 10118 where padding is needed. Examples of such methods are presented in annex B.〕

부록 A 〔Annex A〕
참고 〔informative〕
초기값에 대한 안내〔Guidance on the initializing value〕

초기값은 다양한 방법으로 선택될 수 있다. 예를 들어

- 고정된 값
- 해쉬함수의 매 실행마다 임의로 선택된 값
- 해쉬될 데이터의 성질(길이, 형태 등)에 영향을 받는 값이 될 수 있다. 〔An initializing value can be chosen in a variety of ways: it can, for example, be: - a fixed value; - a value randomly chosen at each execution of the hash-function; - a value depending on one or more characteristics of the data to be hashed(length, type, etc.)〕

이 ISO/IEC 10118 제 1부의 4절은 해쉬코드를 생성하는 실체와 이것을 확인하는 실체가 같은 초기값을 사용하는 것을 보증하기 위해 규정을 만들어야 한다고 되어있다. 이것은 고정된 값을 사용하여도 가능하다. 확인하는 실체에게 초기값이 알려지지 않았을 경우에는 무결성을 보증하는 방법으로 전달되어야 한다. 예를 들어 IV는 해쉬코드와 연결되어 디지탈서명 기법의 입력이 될 수 있다. 〔Clause 4 of this part of ISO/IEC 10118 states that provisions shall be made in order to ensure that the entity which produces the hash-code and the one which checks it use the same initializing value. This can be achieved by using a fixed value. Where the initializing value is not previously known to the checking entity, it is to be conveyed in a manner which ensures its integrity. For example, the IV may be concatenated with the hash-code and input to a digital signature mechanism.〕

부록 B〔Annex B〕
참고 〔(informative)〕
덧붙이기 방법〔Padding methods〕

ISO/IEC 10118의 다른 부분에 상술된 것처럼 해쉬코드를 계산할 때 덧붙이기 방법을 선택해야 하는 경우도 있다. 이 부록에는 두 가지 방법이 제시되어 있다. 해쉬코드가 계산되어져야 하는 데이터의 길이가 해쉬코드의 검증자에게 알려져 있지 않다면 덧붙이기 방법 2가 권고된다. 덧붙이는 비트는 데이터와 같이 저장되거나 보내질 필요가

없다. 검증자는 덧붙이는 비트가 데이터에 포함되었는지 알 수 있다. [The calculation of a hash-code, as specified other parts of ISO/IEC 10118, may require the selection of a padding method. Two methods are presented in this annex. If the length of the data for which the hash-code is to be calculated is not known by a verifier of the hash-code, then padding method 2 is recommended. The padding bits (it any) need not be stored or transmitted with the data. The verifier shall know if the padding bits are included in the data.]

방법 1 [Method 1]

해쉬코드가 계산되어져야 할 데이터는 요구되는 길이를 만들기 위해 필요한 최소한의 길이만큼 '0' 비트로 덧붙여진다. [The data for which the hash-code is to be calculated are appended with as few(possibly no) '0' bits as are necessary to obtain the required length.]

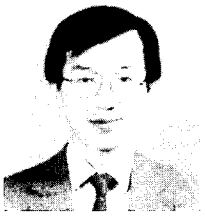
방법 2 [Method 2]

해쉬코드가 계산되어져야 할 데이터는 하나의 '1' 비트로 덧붙여진다. 이렇게 덧붙여진 데이터는 요구되는 길이를 만들기 위해 필요한 최소한의 길이만큼 '0' 비트로 덧붙여진다. [The data for which the hash-code is to be calculated are appended with a single '1' bit. The resulting data are then appended with as few(possible no) '0' bits as are necessary to obtain the required length.]

㈜ 방법 2는 항상 최소한 1비트가 덧붙여진다. [NOTE - Method 2 always requires the addition of at least one padding bit.]

(본 원고를 정리하는 데에 수고를 해준 대학원생 정 경임에게 감사를 표한다.)

□ 著者紹介



이 필 중 (李 弼 中) 종신회원

1951년 12월 30일생
1974년 2월 서울대학교 전자공학과 학사
1977년 2월 서울대학교 전자공학과 석사
1982년 6월 U.C.L.A. System Science, Engineer
1985년 6월 U.C.L.A. Electrical Engineering, Ph.D.
1980년 6월 ~ 1985년 8월 Jet Propulsion Laboratory, Senior Engineer
1985년 8월 ~ 1990년 2월 Bell Communications Research, M.T.S.
1990년 2월 ~ 현재 포항공과대학 전자전기공학과, 부교수