Stateless 해시 기반 서명 기법 동향 및 전망

박태환*, 배봉진*, 김호원*†
*부산대학교 전기전자컴퓨터공학과
e-mail:pth5804@pusan.ac.kr, bongjinbae704@gmail.com,
howonkim@pusan.ac.kr

Stateless Hash-based Signature Scheme Trend and Prospect

Tae-Hwan Park*, Bong-Jin Bae*, Ho-Won Kim*
*Dept of Electric Electronic Computer Engineering, Pusan National University

요 약

최근 양자 컴퓨터 기술의 발전과 양자 컴퓨터와 관련된 Shor 알고리즘과 Grover 알고리즘으로 인해, 기존에 사용되고 있는 블록 암호의 키 크기 증가와 이산대수 기반의 공개키 암호의 안전성에 대한 재평가가 필요한 상황이다. 이러한 상황에서 양자 컴퓨터에 대해 안전한 포스트 양자 암호에 대한 연구가 활발하며, 다변수 기반, 격자 기반, 코드 기반, 해시 기반 등 다양한 포스트 양자 암호들이 연구되고 있다. 본 논문에서는 해시 기반 서명 기법의 경우, 기존의 상태를 활용한 방식의 오랜 연산 시간과 키/서명 크기가 크다는 단점을 가지고 있으며, 이를 개선한 Stateless 해시 기반 서명 기법의 최신 동향과 전망에 대해서 살펴본다.

1. 서론

최근 양자 컴퓨터 기술 발전과 더불어 Shor 알고리즘 및 Grover 알고리즘과 같이 양자 컴퓨터와 관련된 알고리즘들로 인해, 기존에 사용되고 있는 대칭키 암호의 키 사이즈 증가의 필요성과 이산대수 기반의 공개키 암호에 대한 안전성에 대한 재고 및 양자 컴퓨터 환경에서의 안전한 암호 기술 연구 개발이 필요한 상황이다. 이러한 상황에서 많은 암호학자들에 의해 포스트 양자 암호라는 새로운 암호 방식에 대해 연구가 활발히 진행 중이다. 이러한 포스트 양자 암호에는 다변수 기반, 격자 기반, 코드 기반, 해시 기반 등이 있다. 특히 해시 기반의 경우, 암/복호화 기능보다 서명 기법을 제공한다. 해시 기반 서명 기법은 암호학적 해시 함수와 머클 트리(Merkle tree)와 같은 완전이진 트리(Complete binary tree) 구조를 기반으로 하여 기존 RSA, ECDSA 방식과 달리 단일의 공개키/서명키를 사용한 다중 문서 서명/검증을 제공한다. 이러한 해시 기반 서명 기법의 전통적인 방식은 인덱스 기반의 상태를 활용한 방식이다. 이러한 방식은 상태에 따른 많은 정보를 저장해야 되는 단점과 저장과 관련된 많은 연산을 요구한다는 단점을 가지고 있다. 이러한 단점을 극복하기 위해, 상태를 사용하지 않는 Stateless 해시 기반 서명 기법에 대한 다양한 연구가 진행되고 있으며, 32비트의 사물인터넷 디바이스 환경에서도 적용이 가능하다는 장점을 가지고 있다. 본 논문에서는 이러한 Stateless 해시 기반 서명 기법의 동향과 전망에 대해 살펴본다.

본 논문의 구성은 2장에서 Stateful 및 Stateless 해시 기반 서명 알고리즘과 관련된 연구 동향을 살펴보며, 3장에서 Stateless 해시 기반 서명 기법 전망에 대해 살펴본다. 마지막 4장에서 본 논문의 결론을 맺는 순서로 구성된다.

2. 관련 연구 동향

본 장에서는 해시 기반 서명 기법의 전반적인 관련 연구 동향에 대해 살펴본다. 본 장의 구성은 2.1절에서 해시 기반 서명 기법과 관련된 기본 연구동향을, 2.2절에서는 Stateful 해시 기반 서명 기법 관련 연구동향을 살펴보며, 마지막으로 2.3절에서 Stateless 해시 기반 서명 기법 관련 연구동향을 살펴본다.

2.1. 해시 기반 서명 기법 관련 연구 동향

Stateful, Stateless 해시 기반 서명 기법에 대해 살펴보기 전에, 해시 기반 서명 기법과 연관된 연구에 대해 살펴본다.

해시 기반 서명 기법에서 각각의 문서에 대한 서명/검증을 위해, one-time 서명 기법을 사용한다. 본 절에서는 해시 기반 서명 기법에서 사용하는 one-time 서명 기법 중 Lamport-Diffie one-time 서명에 대해 알아본다. Lamport-Diffie one-time 서명은 256bit 크기의 해시 함수를 사용하며, n×2n bit string으로 구성된 서명키와 검증키를 사용한다. 이 때, 균일 랜덤(Uniformly random) 값을 이용해 서명키를 만들고, 서명키와 단 방향

함수를 이용해 검증키를 생성한다[1]. Lamport-Diffie one-time 서명 생성 과정은 문서에 대해, 문서의 메시지 다이제스트 값을 구하고, 해당 다이제스트 값을 인덱스로 하여 서명키로부터 서명 값을 생성한다. 이후 Lamport-Diffie one-time 서명 검증 과정에서 단 방향 함수와 검증키 값을 이용해 생성한 값과 검증키 값을 비교하여 서명 검증을 하게 된다. 이러한 Lamport-Diffie one-time 서명의 경우, 연산이 매우 효율적이라는 장점을 가지지만, 서명의 크기가 매우 크다는 단점을 가지고 있다. 이러한 문제점을 해결하기 위해 메시지 다이제스트의 일부 비트를 동시에 서명하는 Winternitz one-time 서명이 제안되었다[1]. Winternitz one-time 서명에 있어서 동시에 서명하고자하는 비트 수를 나타내는 Winternitz parameter(w)를 2 이상의 수로 선택한 후, 선택된 Winternitz parameter(w)를 기반으로 t라는 값을 구한다. 이후 균일 랜덤(Uniformly random)값을 이용해 서명키를 생성하되, Lamport-Diffie one-time 서명에서 n×2n bit 길이였던 서명키를 n×t bit로 감소시켜 생성한다. 그리고 검증키를 생성할 때는 서명키와 2^w-1회 만큼 단 방향 함수를 사용해 검증키를 생성한다.

Winternitz one-time 서명 생성 과정은 문서에 대한 메시지 다이제스트 값의 길이가 Winternitz parameter(w)에 의해 나누어 질 수 있도록 0을 최소한의 개수로 값 앞에 패딩 하고, 패딩된 메시지 다이제스트를 특정 크기로 나눈 다음 나누어진 값(b_i)을 이용해 checksum(c)을 구한다. 이후 서명키를 checksum(c) 횟수만큼 단 방향 함수를 사용해 서명 값을 생성한다.
서명 검증 과정은 서명 값을 2^w-1-b_i회 만큼 단 방향 함수를 사용해 생성된 값과 검증 값을 비교하여 서명 검증을 하게 된다.

이러한 Winternitz one-time 서명(WOTS)의 변형으로는 $WOTS^{\$}$, $WOTS^{+}$가 있다.

2.2. Stateful 해시 기반 서명 기법 관련 연구

Stateful 해시 기반 서명 기법의 가장 기본이 되는 머클 트리 서명 기법(Merkle tree Signature Scheme, MSS)은 머클 트리(Merkle tree) 구조를 사용하여 트리의 높이인 H에 따라 2^H개의 문서에 대한 서명/검증이 가능하다. 머클 트리 서명 기법(Merkle tree Signature Scheme, MSS)에서의 공개키는 머클 트리(Merkle tree)의 root에 위치하며, 2^H개의 개인키(서명키)는 leaf 노드에 위치한다. i번째 Leaf 노드에는 각각의 문서에 대한 개인키(서명키) 및 문서의 다이제스트 값을 가지고 있으며, 머클 트리(Merkle tree)의 inner 노드는 자신의 왼쪽, 오른쪽 자식 노드의 Concatenation 결과에 대한 해시 값을 가진다[1].

Merkle tree의 서명키/검증키 생성 과정은 총 2^H개의 Winternitz one-time 서명키/검증키 쌍을 생성하며, 2^{H+1}-1회의 해시 함수 수행이 필요하다. 특히 머클 트리(Merkle tree)의 root에 위치한 공개키에 대한 효율적인 생성을 위해서 트리해시(Treehash) 알고리즘을 사용해 최대 H개의 트리 노드만 저장함으로써 메모리 사용의 효율성을 높일 수 있다[1].

Rohde, Sebastian, et al.[2]에서는 8비트 스마트카드 환경 상에서의 MSS(Merkle signature scheme) 구현 결과를 제시하며, Buchmann, Johannes, et al.[3]에서는 MSS 기법을 좀 더 효율적으로 개선한 CMSS를 제안하였으며, Java 기반의 구현 결과를 제시하고 있다. De Oliveira method.[4]에서는 multi-buffer 기법 기반의 State 해시 기반 서명 기법의 고속화 결과를 제시하고 있다. Eisenbarth, Thomas, et al.[5]은 AVR-ATxmega 계열 보드 상에서의 state 해시 기반 서명 기법의 고속 구현 결과를 제시하고 있으며, Hulsing, Andreas, et al.[6]에서는 CMSS의 확장버전인 XMSS와 Multi-tree XMSS 등과 같은 알고리즘을 제안하고 있으며, 현재 XMSS의 경우, IETF 표준화 진행 중에 있다.

2.3. Stateless 해시 기반 서명 기법 관련 연구

앞서 살펴본 State 해시 기반 서명 기법의 경우, 상태 기반의 연산으로 인한 많은 메모리 소모 및 추가적인 연산이 필요하다는 단점과 순차적인 연산이 필요하다는 단점을 가지고 있다. 이러한 문제점을 해결하기 위해, 상태를 사용하지 않는 stateless 해시 기반 서명 기법에 대한 연구가 활발히 이루어지고 있다.

본 절에서는 stateless 해시 기반 서명 기법에 대한 연구 동향에 대해 살펴본다. Oded, Goldreich method[7]는 인덱스에 대한 랜덤 값을 활용하는 방식의 stateless 해시 기반 서명 기법에 대한 제시하였다. 제시한 기법은 Winternitz 파라미터(w)를 16으로 설정하였으며, 높이가 256인 머클 트리(Merkle tree)를 사용하여 0.6MB의 서명을 생성하였다. 하지만 서명의 크기가 아직 응용 서비스에 적용하기에는 크다는 단점을 가지고 있으며, 이러한 문제점을 해결하기 위해, Bernstein, Daniel J., et al.[8]은 hyper-tree 자료구조와 few-time signature 기법을 적용하는 SPHINC라는 stateless 해시 기반 서명 기법을 제안하였다. 제안된 기법을 기반한 SPHINCS-256은 양자 컴퓨터 환경에서 128비트의 보안강도를 제공하며, Winternitz 파라미터(w) 16을 사용하고, BLAKE-512를 해시함수로 사용하며, ChaCha12를 PRG로 사용하였다. 해당 논문에서는 인텔 프로세서 환경에서 AVX2 기반의 SIMD(Single Instruction Multiple Data) 구현 결과를 제시하고 있으며, 41KB의 서명과 1KB 크기의 공개키/비밀키를 제공할 수 있다. 이 결과는 Oded, Goldreich method[7]의 서명 크기에 약 15배 정도 작은 크기의 해시 기반 서명을 제공할 수 있다.

Hülsing, Andreas et al.[9]의 경우, 앞서 설명한 SPHINCS-256을 ARM Cortex-M3 프로세서 환경

상에서의 구현 결과를 제시하고 있다.

3. Stateless 해시 기반 서명 기법 전망

2장에서 살펴본 바와 같이 최근에 Stateless 해시 기반 서명 기법에 대한 연구가 활발히 진행되고 있으며, 실제 적용과 관련 표준화가 필요한 상황이다. 이를 위해, 앞으로 다양한 해시 함수와 PRG 적용을 통한 최적화 연구, 다양한 환경에서의 적용 연구, 그리고 서명 및 키 크기에 대한 최적화 연구가 필요한 상황이다. 표준화의 경우, 현재 미국 NIST의 포스트 양자 암호 표준 공모 사업이 진행되고 있으며, 이에 대한 준비 및 각국에서의 표준화와 관련 제도 마련이 시급한 상황이다. 이러한 최적화 및 응용 연구와 더불어 표준화/제도 연구가 활발히 이루어질 것이라고 예상된다.

4. 결론

본 논문에서는 포스트 양자 암호 중 하나인 해시 기반 서명 기법에서의 최신 연구 동향인 Stateless 해시 기반 서명 기법에 대한 연구 동향과 전망에 대해 살펴보았다. 기존의 Stateful 해시 기반 서명 기법의 경우, 상태(state)에 따른 정보 저장과 부가적인 연산이 필요하다는 단점을 가지고 있으며, 이를 해결하기 위한 방안으로 Stateless 해시 기반 서명 기법 연구가 활발히 이루어지고 있으나, 아직 실용화하기에는 서명 크기가 크며, 속도가 느리다는 단점이 있다. 이에 대해 최적화 연구를 통한 실용화가 필요한 상황이며, 해시 기반 서명 기법에 대한 표준화 및 제도화 연구가 필요한 상황이다. 앞으로 이러한 방향으로 연구가 활발히 이루어질 것이라고 예상된다. 본 논문에서 살펴본 동향과 전망은 앞으로의 해시 기반 서명 기법에 대한 연구를 위한 기초 자료로 사용할 수 있을 것으로 생각된다.

감사의 글

이 논문은 2016년도 정부(미래창조과학부)의 재원으로 정보통신기술진흥센터의 지원을 받아 수행된 연구임 (R0101-16-0129, 개방형 고성능 표준 IoT 디바이스 및 지능형 SW 개발)

참고문헌

[1] Bernstein, Daniel J., Johannes Buchmann, and Erik Dahmen, eds. Post-quantum cryptography. Springer Science & Business Media, 2009

[2] Sebastian Rohde, Fast Hash-Based Signatures on Constrained Devices, CARDIS 2008, p.104-117, 2008

[3] Johannes Buchmann, CMSS - An Improved Merkle Signature Scheme, Progress in Cryptology - INDOCRYPT, p.349-363, 2006

[4] Ana Karina D.S. de Oliveira, An Efficient Software Implementation of the Hash-Based Signature Scheme MSS and Its Variants, LATINCRYPT 2015, p.366-383, 2015

[5] Thomas Eisenbarth, A Performance Boost for Hash-based Signatures, LNCS 8260, p.166-182, 2013

[6] Andreas Hülsing, Hash-based Signatures: An Outline for a New Standard, 2015

[7] Oded, Goldreich. "Foundations of Cryptography: Volume 2, Basic Applications." (2009).

[8] Bernstein, Daniel J., et al. "SPHINCS: practical stateless hash-based signatures." Advances in Cryptology-EUROCRYPT 2015. Springer Berlin Heidelberg, 2015. 368-397.

[9]Hülsing, Andreas, Joost Rijneveld, and Peter Schwabe. "ARMed SPHINCS Computing a 41KB signature in 16KB of RAM." (2016).