동적집단에 대한 턱값RSA서명규약

김경훈, 송현준

경애하는 최고령도자 **김정은**동지께서는 다음과 같이 말씀하시였다.

《우리 나라를 과학기술강국의 지위에 올려세우기 위하여서는 인재를 중시하며 전민과학기술인재화를 실현하여야 합니다.》(《조선로동당 제7차대회에서 한 중앙위원회사업총화보고》 단행본 41페지)

론문에서는 학적자료에 대한 보안을 동적집단에 대한 턱값RSA서명규약을 리용하여 분산서명을 진행하여 보안강도를 높이기 위한 한가지 방법을 제안하였다.

1. 분산서명에 대한 정의

수자서명은 통보문의 완전성과 신분인증, 부인불가능성을 담보하는 강력한 도구[1]라고 할수 있다.

만일 통보 M과 n명의 가입자모임이 주어졌을 때 매 가입자가 비밀열쇠의 한 부분을 소유한다고 하자.

이때 임의의 t명이상의 가입자들이 M에 대한 서명을 생성할수 있으면 분산서명방식을 (t, n)턱값서명방식[2]이라고 부른다. 체계가 많은 통보들에 대한 서명들을 생성하였을 때에도 t명(혹은 더 적은)의 가입자들이 새로운 통보에 대한 서명을 생성할수 없으면 그 방식은 안전하다 혹은 위조불가능하다[2]고 말한다. 또한 (t, n)턱값서명방식이 t명까지의 임의의 비법가입자들의 존재시에도 서명들을 정확히 계산할수 있으면 그 방식을 견딤성(혹은 결점견딤)[2]이라고 부른다.

2. 동적집단에 대한 턱값RSA서명규약

론문에서는 서명열쇠와 서명검증열쇠가 갱신된 후 생명주기동안에 신뢰되는 가입자가 없이 임의의 가입자가 부분서명기능을 부여받거나 이미 권한을 가진 가입자들이 빠질수 있는 동적집단에 대한 RSA서명규약구성문제에 대하여 제안하였다.

권한을 가진 $t+1$명 가입자들의 모임 B로부터 새로운 가입자 $p_{u'}$에게 집단서명에 참가할수 있는 권한을 주는 규약은 다음과 같다.

규약 1 새로운 가입자에 대한 비밀분할

단계 1 매 가입자 p_{u_i}, $i \in N_{t+1}^{+}$는 값 $d_{u_i}(u')$를 계산하여 $p_{u'}$에게 비밀리에 전송한다.

단계 2 가입자 $p_{u'}$는 $e^{-1} \bmod \phi$에 관한 자기의 분할몫을 다항식 $d_{u'}(x)$로, $d(0, u')$를 자기의 부분서명열쇠로 가진다.

권한가진 매 가입자 p_u는 비밀분할몫으로 $\tilde{d}(x, u) = \delta_u d(x, u)$가 성립하는 $\tilde{d}(x, u)$와 추가적인 값 δ_u를 소유한다.

규약 2 옹근수우에서의 새 가입자에 대한 비밀분할

단계 1 매 가입자 p_{u_i}, $i \in N_{t+1}^{+}$는 $\tilde{d}_{u_i}(u') = \tilde{d}(u', u_i)$와 δ_{u_i}를 가입자 $p_{u'}$에게 비밀리에 전송한다.

단계 2 $\delta = \mathrm{lcm}\{\delta_{u_1}, \cdots, \delta_{u_{t+1}}\}$로 놓고

$$\tilde{d}_{u'}(x) = \tilde{d}(x, u') = \delta_{\Delta_B} d(x, u') = \delta_{\Delta_B} \sum_{i=1}^{t+1} L_B(x, u_i) \frac{\tilde{d}(u', u_i)}{\delta_{u_i}}$$

를 계산한다.

단계 3 다항식 $\tilde{d}_{u'}(x)$와 $\delta_{u'} = \delta_{\Delta_B}$를 자기의 분할몫으로 보관한다.

규약 2에 토대하여 분할몫을 가진 권한이 부여된 $t+1$명의 가입자들의 모임 $B' = \{u_1, u_2, \cdots, u_{t+1}\}$에 대하여 부분서명에 의한 집단서명을 수행하는 턱값RSA부분서명을 다음과 같이 요약할수 있다.

규약 3 동적집단에 대한 서명규약

단계 1 매 가입자 $P_u \in B'$는 자기의 비밀분할몫을 가진 자기의 부분서명 $\sigma_{u_i} = y^{\tilde{d}(0, u_i)}$을 계산하여 쌍 $(\sigma_{u_i}, \delta_{u_i})$를 제출한다.

단계 2 우선 $t+1$개의 부분서명들로부터 집단서명을 다음과 같이 계산한다.

$$\Delta_{B'} = \mathrm{lcm}\left\{\prod_{i=1}^{t+1}(u_i - u_j),\ i \in N_{t+1}^{+}\right\}$$

다음 $\delta = \mathrm{lcm}\{\delta_{u_1}, \cdots, \delta_{u_{t+1}}\}$을 계산하고 $\alpha e + \beta \Delta_{B'} = 1$이 성립하는 옹근수 α, β를 구한다.

단계 3 $\sigma = y^{\alpha}\left[\prod_{i=1}^{t+1}(\sigma_{u_i})^{\frac{\delta}{\delta_{u_i}} L_B(0, u_i)}\right]^{\beta} \bmod N$을 계산하여 집단서명으로 출력한다.

구성한 규약은 모두 옹근수우에서 연산이 효과적으로 진행된다.

맺 는 말

가입자들이 임의로 변할수 있는 동적집단에서의 안전하고 효률적인 검증가능한 분산서명체계를 구성하고 그것의 안전성론의를 진행하였으며 그것을 리용하여 학적자료에 대한 분산서명체계를 확립함으로써 학적자료에 대한 공정성과 정확성, 완전성을 더욱 확고히 담보할수 있게 하였다.

참 고 문 헌

[1] 김영진; 암호학적정보보호, **김일성**종합대학출판사, 221～245, 주체104(2015).

[2] Rosario Gennaro et al.; Advances in Cryptology-Eurocrypt, 88, 2008.

주체107(2018)년 2월 5일 원고접수

Threshold RSA Signature Protocol for Dynamic and Ad-Hoc Groups

Kim Kyong Hun, Song Hyon Jun

In this paper, we proposed the schemes that provided the efficient and flexibility required in ad-hoc groups, and the capability of incorporating new members to the group of potential signers without relying on central authorities.

Key words: threshold cryptography, distributed signature, threshold signature