(19) 대한민국특허청(KR)
(12) 공개특허공보(A)

(11) 공개번호 10-2012-0072014
(43) 공개일자 2012년07월03일

(51) 국제특허분류(Int. Cl.)
H04L 9/32 (2006.01) *G06Q 20/40* (2012.01)
G06F 21/20 (2006.01)
(21) 출원번호 10-2010-0133776
(22) 출원일자 2010년12월23일
심사청구일자 없음
기술이전 희망 : **기술양도, 실시권허여, 기술지도**

(71) 출원인
한국전자통신연구원
대전광역시 유성구 가정로 218 (가정동)
(72) 발명자
배근태
대전광역시 서구 둔산대로117번길 66, 908호 (만년동, 골드타워)
황정연
경기도 수원시 권선구 세지로12번길 25-10, 대우연립 10동 201호 (세류동)
(뒷면에 계속)
(74) 대리인
김원준, 제일특허법인

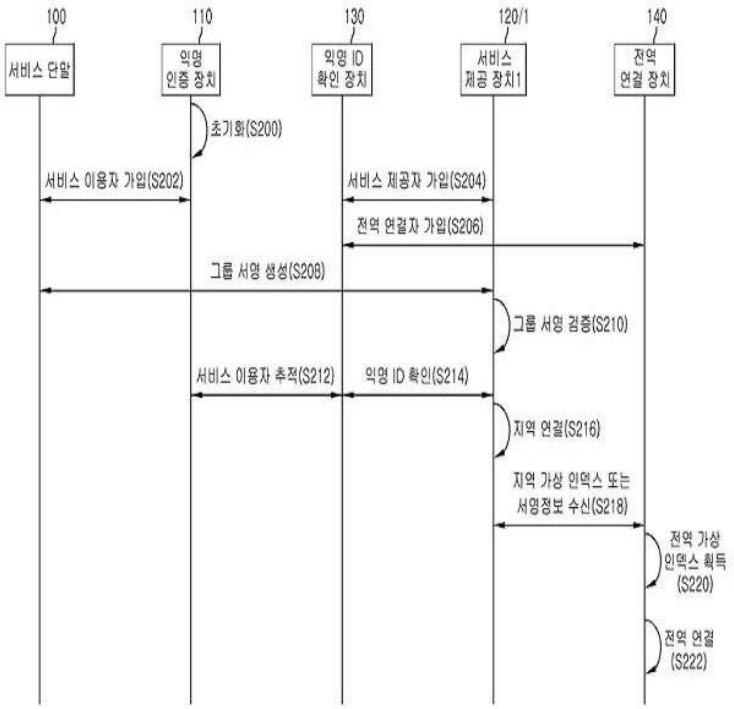
전체 청구항 수 : 총 20 항

(54) 발명의 명칭 **익명 인증 서비스 방법**

(57) 요 약

불연계성(Unlinkability)을 단순히 일반적인 인터넷 서비스에 적용할 경우 매우 불편할 수 있다. 서비스제공자는 일반적으로 서비스 이용 관련 통계를 내고 이 통계를 바탕으로 서비스 전략을 세우고, 또한 단골 서비스 이용자, 불량 서비스 이용자 등을 구분하여 이들에게 특화된 서비스를 제공하거나 서비스 이용에 제약을 가하는 등의 다양한 서비스를 제공하여야 하는데, 익명 인증 기법에 따르면 서비스 이용자에 대한 정보를 전혀 얻을 수 없어 서비스 계획과 전략을 수립하기 어렵게 되기 때문이다. 이에 본 발명의 실시예에서는, 계층적 연결성(Hierarchical Linkability)이라는 새로운 개념을 제안하고자 한다. 계층적 연결성은 연결성 정보의 확인 과정을 계층화 시켜 상위의 권한을 가진 경우 더 넓은 범위의 연결성을 확인할 수 있다. 이를 통해 지역 연결성(Local Linkability)은 물론 전역 연결성(Global Linkability) 정보를 제어할 수 있다. 그리고, 이를 이용하여 적정한 수준의 익명성을 보장하면서도 효과적인 익명 회원 관리가 가능한 익명 서비스 방법을 제공하고자 한다.

대 표 도



(72) 발명자

이석준

대전광역시 유성구 배울1로 119, 대덕테크노밸리 우림필유 1207동 1102호 (용산동)

이상우

대전광역시 유성구 배울2로 78, 대덕테크노밸리아파트 603동 804호 (관평동)

이윤경

대전광역시 유성구 배울2로 19, 대덕테크노밸리 꿈에그린아파트 910동 1202호 (관평동)

김신효

대전광역시 유성구 엑스포로 448, 404동 1106호 (전민동, 엑스포아파트)

정병호

대전광역시 유성구 가정로 65, 102동 1305호 (신성동, 대림두레아파트)

문혜란

경기도 광주시 경충대로 1514-11, 이스트빌 3동 402호 (쌍령동)

조현숙

대전광역시 유성구 관평1로 12, 702동 601호 (관평동)

이 발명을 지원한 국가연구개발사업

과제고유번호	KI001917
부처명	지식경제부
연구사업명	정보통신산업원천기술개발사업
연구과제명	익명성 기반의 u-지식 정보보호 기술 개발
주관기관	한국전자통신연구원
연구기간	2010.03.01 ~ 2011.02.28

특허청구의 범위

청구항 1

익명 ID 확인 장치로부터 서비스 제공 장치의 전역 연결키(Global Link Key)를 수신하는 과정과,

상기 서비스 제공 장치로부터 서비스 단말의 서명정보 또는 지역 가상 인덱스를 수신하는 과정과,

수신되는 상기 전역 연결키를 통해 상기 서명정보의 전역 가상 인덱스를 획득하여 상기 서비스 단말의 전역 연결성 정보를 확보하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 2

제 1 항에 있어서,

상기 전역 연결키를 수신하는 과정은,

상기 서비스 단말이 인명 인증 장치와 상호 협력하여 상기 서비스 단말의 사용자의 서명 비밀키를 획득하는 과정과,

상기 서비스 제공 장치가 상기 익명 ID 확인 장치와 상호 협력하여 상기 서비스 제공 장치의 공개키 및 비밀키쌍을 획득하는 과정과,

상기 서비스 제공 장치의 상위에서 전역 연결정보를 관리하고자 하는 전역 연결 장치가 상기 익명 ID 확인 장치와 상호 협력하여 상기 서비스 제공 장치의 상기 전역 연결키를 제공받는 과정을 포함하는

익명 인증 서비스 방법.

청구항 3

제 2 항에 있어서,

상기 지역 가상 인덱스를 수신하는 과정은,

상기 서비스 단말이 상기 서비스 제공 장치로부터 상기 공개키를 제공받고, 상기 공개키와 상기 서명 비밀키를 기반으로 하여 상기 서비스 단말의 사용자 서명을 생성하는 그룹서명 생성 과정과,

상기 서비스 제공 장치가 상기 사용자 서명의 유효 여부를 검증하는 그룹서명 검증 과정과,

상기 익명 ID 확인 장치가 상기 사용자 서명으로부터 익명ID를 계산한 후, 상기 익명 인증 장치와 상호 협력하여 상기 익명ID를 가지는 서비스 이용자를 확인하는 서명자 확인 과정과,

상기 서비스 제공 장치가 상기 공개키를 통해 상기 사용자 서명의 정당성 여부를 확인하고, 상기 비밀키를 통해 상기 사용자 서명으로부터 상기 서비스 단말의 가상 인덱스를 획득하여 상기 서비스 단말의 지역 연결성을 확보하는 지역연결 과정을 포함하는

익명 인증 서비스 방법.

청구항 4

제 2 항에 있어서,

상기 전역 연결성 정보를 확보하는 과정은,

상기 전역 연결 장치가 상기 서비스 제공 장치로부터 상기 서비스 단말의 상기 지역 가상 인덱스 또는 서명정보를 제공받는 과정과,

상기 전역 연결 장치가 상기 전역 연결키를 통해 상기 전역 가상 인덱스를 획득하여 상기 서비스 단말의 전역 연결성 정보를 확보하는 전역 연결 과정을 포함하는

익명 인증 서비스 방법.

청구항 5

제 2 항에 있어서,

상기 서명 비밀키를 획득하는 과정은,

상기 서비스 단말이 상기 사용자의 개인키 소유 증명 정보와 신원확인정보를 상기 익명 인증 장치로 제공하는 과정과,

상기 익명 인증 장치가 상기 서비스 단말의 사용자에 대응되는 익명ID를 포함하는 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정과,

상기 서비스 단말의 사용자를 등록하는 과정과,

상기 서비스 단말이 상기 그룹 멤버키에 대응되는 상기 서명 비밀키를 생성하여 저장하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 6

제 5 항에 있어서,

상기 그룹 멤버키는, $(\hat{A}_i, x_i, z_i)$ ($\hat{A} = (\hat{g}_1 \hat{g}_4^{-z_i} \hat{g}_3^{-y_i})^{1/(\gamma+x_i)} \in G_1$ 및 $y_i, x_i, z_i \in \mathbb{Z}_p^*$ 및 바이리니어 그룹 G_1, G_2 및 $g_1 = \varphi(g_2)$ 및 동형함수 φ 및 $g_2 \in G_2 \setminus \{1_{G_2}\}$ 및 $g_3, g_4 \in G_1 \setminus \{1_{G_1}\}$ 및 $\gamma \in \mathbb{Z}_p^*$ 및 해시함수 $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$ 로 표현되고,

상기 서명 비밀키는 $gsk[i] = (\hat{A}_i, x_i, z_i, y_i)$ 로 표현되며,

상기 개인키 소유 증명 정보는 $g_3 \in G_1$ 에 대해 y_i 를 소유하고 있다는 증명 정보인 것을 특징으로 하는

익명 인증 서비스 방법.

청구항 7

제 5 항에 있어서,

상기 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정은,

상기 서비스 단말의 사용자가 이미 등록되어 있는 경우, 상기 서비스 단말의 사용자에 대응되는 상기 그룹 멤버키를 갱신하여 상기 서비스 단말로 제공하는 과정과,

상기 서비스 단말의 사용자가 미등록되어 있는 경우, 상기 서비스 단말의 사용자에 대응되는 상기 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정과,

상기 서비스 단말의 사용자를 등록하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 8

제 5 항에 있어서,

상기 등록하는 과정은,

상기 서비스 제공 장치가 서비스 제공자의 신원확인정보를 상기 익명 ID 확인 장치로 제공하는 과정과,

상기 익명 ID 확인 장치가 상기 서비스 제공자에 대응되는 상기 공개키 및 비밀키쌍과 추적키를 생성하여 상기 서비스 제공자를 등록하고, 상기 공개키 및 비밀키쌍을 상기 서비스 제공 장치로 제공하는 과정과,

상기 서비스 제공 장치가 상기 공개키 및 비밀키쌍으로부터 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 9

제 8 항에 있어서,

상기 공개키는, (h_j, m_j, u_j, v_j) ($h_j = m_j^{x_j}$, $u_j = m_j^{\xi_{1j}}$, $v_j = m_j^{\xi_{2j}} \in G_1$, $m_j \in G_1 \setminus \{1_{G_1}\}$, $x_j, \xi_{1j}, \xi_{2j} \in \mathbb{Z}_p^*$, $H : \{0,1\}^* \rightarrow \mathbb{Z}_p$, H는 해쉬함수, G_1 은 바이리니어 그룹)으로 표현되고,

상기 SP 공개키는 $gpk_{SP}[j] = (e, G_1, G_2, \hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4, \hat{w}, h_j, m_j, u_j, v_j)$ (e 는 동형함수, G_2 는 바이리니어 그룹, $g_1 = \varphi(g_2)$, $g_2 \in G_2 \setminus \{1_{G_2}\}$, $g_3, g_4, h \in G_1 \setminus \{1_{G_1}\}$, $w = g_2^{\gamma} \in G_2$, $\gamma \in \mathbb{Z}_p^*$)으로 표현되며,

상기 비밀키는 (M_j, U_j, V_j) ($M_j \in G_2 \setminus \{1_{G_1}\}$, $U_j = M_j^{\xi_{1j}}$, $V_j = M_j^{\xi_{2j}} \in G_2$)으로 표현되고,

상기 추격키는 ($tk_{sp}[j] = (\xi_{1j}, \xi_{2j}, x_j)$)($x_j, \xi_{1j}, \xi_{2j} \in \mathbb{Z}_p^*$)으로 표현되는 것을 특징으로 하는

익명 인증 서비스 방법.

청구항 10

제 9 항에 있어서,

상기 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정은,

상기 서비스 제공 장치가 현재 세션의 그룹 공개 파라메터를 이용하여 상기 공개키로부터 상기 SP 공개키를 생성하고 저장하는 과정과,

상기 서비스 제공 장치가 상기 비밀키를 상기 LL 비밀키로 저장하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 11

제 10 항에 있어서,

상기 그룹 공개 파라메터는 ($gpk = (e, G_1, G_2, g_1, g_2, g_3, g_4, w)$)로 표현되며,

상기 SP 공개키는 ($gpk_{SP}[j] = (e, G_1, G_2, \hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4, \hat{w}, h_j, m_j, u_j, v_j)$)로 표현되는 것을 특징으로 하는

익명 인증 서비스 방법.

청구항 12

제 10 항에 있어서,

상기 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정은,

상기 SP 공개키를 생성하고 저장하는 과정과 상기 LL 비밀키로 저장하는 과정을 수행하기 전에, 상기 서비스 제공 장치가 공개키 및 비밀키쌍이 $e(m_j, M_j) = e(u_j, U_j) = e(v_j, V_j)$ 의 식을 만족하는지를 확인하는 과정을 더 포함하는

익명 인증 서비스 방법.

청구항 13

제 2 항에 있어서,

상기 전역 연결키를 수신하는 과정은,

상기 전역 연결 장치가 전역 연결자의 신원확인정보를 상기 익명 ID 확인 장치에 제공하는 과정과,

상기 익명 ID 확인 장치가 상기 전역 연결자를 등록하는 과정과,

하위 서비스 제공 장치의 상기 전역 연결키를 상위 서비스 제공 장치로 제공하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 14

제 13 항에 있어서,

상기 상위 서비스 제공 장치는 상기 전역 연결 장치이며, 상기 하위 서비스 제공 장치는 다수의 서비스 제공 장치들을 포함하는

익명 인증 서비스 방법.

청구항 15

제 13 항에 있어서,

상기 전역 연결키는, 상기 하위 서비스 제공 장치에 대하여 수학식 $LK_j = rb_j^{-1}$ (하위 서비스 제공 장치 j의 경우)로 표현되는

익명 인증 서비스 방법.

청구항 16

제 15 항에 있어서,

상기 전역 연결 장치는, 상기 수학식 $LK_j = rb_j^{-1}$ 을 통해 상기 전역 가상 인덱스를 제공받는

익명 인증 서비스 방법.

청구항 17

제 13 항에 있어서,

상기 전역 연결키는, 상기 하위 서비스 제공 장치에 대하여 수학식 $(U_j = M^{t_{1,j}}, V_j = M^{t_{2,j}}, M)$ (서비스 제공 장치 j의 경우)로 표현되는

익명 인증 서비스 방법.

청구항 18

제 17 항에 있어서,

상기 전역 연결 장치는, 상기 수학식 $(U_j = M^{t_{1,j}}, V_j = M^{t_{2,j}}, M)$ 을 통해 상기 서명정보를 제공받는

익명 인증 서비스 방법.

청구항 19

제 3 항에 있어서,

상기 그룹서명 생성 과정은,

상기 서비스 단말이 상기 서비스 제공 장치로부터 서비스 제공자의 SP 공개키를 획득하는 과정과,

상기 서비스 단말이 상기 SP 공개키 및 상기 서명 비밀키 및 메시지를 이용하여 상기 사용자 서명을 생성하는 과정을 포함하는

익명 인증 서비스 방법.

청구항 20

제 3 항에 있어서,

상기 서명자 확인 과정은,

상기 익명 ID 확인 장치가 상기 추적키를 이용하여 상기 사용자 서명으로부터 상기 서비스 이용자의 익명 ID를 추출하는 과정과,

상기 익명 ID 확인 장치가 상기 익명 인증 장치와 상호 협력하여 상기 익명ID에 대응되는 신원확인정보 및 상기 그룹 멤버키를 갖는 서비스 이용자를 확인하는 과정을 포함하는

익명 인증 서비스 방법.

명 세 서

기 술 분 야

[0001] 본 발명은 그룹서명 기법(Group Signature)을 이용하여 익명성을 유지하면서도 제어 가능한 계층적 연결성을 제공하는 인증(anonymity) 기술에 대한 것으로, 특히 지역 연결키(Local Link Key)가 주어진 경우에는 동일한 서비스 도메인 내에서만 그룹 서명 값들에 대한 연결성이 확인가능하며 전역 연결키(Global Link Key)가 주어진 경우에는 서비스 도메인들에 상관없이 그룹 서명 값들에 대한 연결성을 확인할 수 있는 전역 연결성을 제공하는데 적합한 익명 인증 서비스 기술에 관한 것이다.

배 경 기 술

[0002] 편리한 인터넷 상의 응용을 위해서 개인의 중요한 정보가 다루어진다. 인터넷 뱅킹 등의 금융 거래 등에 대

해 실명 확인 및 서명을 하거나, 특정 서비스를 이용하기 위한 실명 확인 및 인증을 위하여 PKI(Public Key Infrastructure) 기반 전자인증서를 사용한다. PKI 기반 전자인증서는 그 비밀키를 소유한 사람만이 전자 서명을 생성할 수 있으며, 비밀키를 소유하지 않은 사람이 전자 서명을 위조할 확률이 무시 가능한 정도로 매우 낮기 때문에 매우 안전하면서 편리한 전자 서명 및 인증이 가능하도록 해준다. 그러나, 대체로 공인인증기관에 의해 발행된 인증서에는 사용자 실명이 그대로 드러나며, 주민등록번호와 같은 중요한 개인정보가 일치하는지를 암호학적으로 확인할 수 있는 정보 등도 포함되어 있으므로, 특정 전자 서명 정보를 누가 생성했는지를 쉽게 알 수 있어 개인의 프라이버시 문제를 야기할 수 있다. 또한, 원활한 서비스를 제공하고 동시에 서비스 제공자는 다양한 서비스 개발을 위해 많은 개인 정보를 요구한다. 하지만, 개인정보의 등록 및 확인 과정을 통해 개인정보 노출, 서비스 제공자의 과도한 개인정보 수집 및 관리 부주의로 인한 유출 등과 같은 많은 잠재적인 또는 실제적인 문제점을 나타내고 있다.

[0003] 이러한 프라이버시 문제를 해결하고 양질의 개인화된 서비스 제공을 위해서 최근 익명인증 기법 등이 활발히 연구되고 있다. 프라이버시 제공을 위한 제공해야 할 기본적인 특성 중 하나로 불연계성(Unlinkability)이 있다. 불연계성은 익명 사용자가 익명 인증을 여러 번 수행 하였을 때, 검증자(대체로, 서비스제공서버)가 이들이 같은 사용자인지 아닌지를 판단할 수 없음을 의미한다. 만약 불연계성 기능이 제공되지 않는다면, 특정 사용자의 서비스 이용 패턴 및 이용 기록이 추적(tracking) 가능해진다. 이러한 기록을 바탕으로 사용자의 익명성이 훼손되거나 특정 기록 중 한군데서 실명이 노출될 경우, 전체적인 익명성이 깨지게 된다.

[0004] 그러나, 불연계성을 단순히 일반적인 인터넷 서비스에 적용할 경우 매우 불편할 수 있다. 서비스제공자는 일반적으로 서비스 이용 관련 통계를 내고 이 통계를 바탕으로 서비스 전략을 세우고, 또한 단골 서비스 이용자, 불량 서비스 이용자 등을 구분하여 이들에게 특화된 서비스를 제공하거나 서비스 이용에 제약을 가하는 등의 다양한 서비스를 제공하여야 하는데, 익명 인증 기법에 따르면 서비스 이용자에 대한 정보를 전혀 얻을 수 없어 서비스 계획과 전략을 수립하기 어렵게 되기 때문이다.

[0005] 따라서, 사용자의 프라이버시 강도를 일부 완화시키지만, 상기와 같은 요구 사항을 만족시킬 수 있는 새로운 방식의 익명 서비스 방법의 필요성이 대두되고 있다. 특히, 위와 같은 서비스 고려시, 체계적으로 연계성을 통제할 수 있다면 많은 응용 분야에서 익명 인증 기법이 유용하게 사용될 수 있을 것이다.

발명의 내용

해결하려는 과제

[0006] 이에 본 발명의 실시예에서는, 계층적 연결성(Hierarchical Linkability)이라는 새로운 개념을 제안하고자 한다.

[0007] 계층적 연결성은 연결성 정보의 확인 과정을 계층화 시켜 상위의 권한을 가진 경우 더 넓은 범위의 연결성을 확인할 수 있다. 이를 통해 지역 연결성(Local Linkability)은 물론 전역 연결성(Global Linkability) 정보를 제어할 수 있다. 그리고, 이를 이용하여 적정한 수준의 익명성을 보장하면서도 효과적인 익명 회원 관리가 가능한 익명 서비스 방법을 제공하고자 한다.

[0008] 연결성 정보 확인의 수준을 계층화 시키면, 서비스 제공자들의 서비스 이용자들에 대한 연결성 요구 수준이 계층화되어 있는 경우 유용하게 활용할 수 있다. 서비스 이용자가 상위의 지불 게이트웨이(PG: Payment Gateway)를 통하여 하위의 여러 서비스 제공자에 대한 지불 서비스를 받는 것이 한 예가 될 수 있다. 이 경우, 각각의 하위 서비스 제공자들이 지역 연결성 정보를 통하여 다양한 서비스를 제공하되, 사용자의 지불 정보는 전역적인 연결성을 통하여 관리되어야 하므로 상위에 전역 연결자(Global Linker)(지불 게이트웨이)를 두어 전역 연결성 정보를 제어할 수 있도록 한다.

[0009] 이때, 하위의 서비스 제공자들과 상위의 전역 연결자 모두에 대해 서비스 이용자의 익명성이 유지되지만, 하위 서비스 제공자들은 각각의 도메인 범위에서 연결성 정보를 확인할 수 있고, 상위의 전역 연결자는 이러한 하위 서비스 제공자들을 모두 감싸는 범위의 상위 도메인에 대하여 연결성 정보를 확인할 수 있게 된다.

[0010] 본 발명의 구성으로 인해, 지불 게이트웨이를 통한 지불서비스 등에서 서비스 제공자들의 서비스 이용자들에 대한 연결성 서비스를 유용하게 활용할 수 있다.

과제의 해결 수단

[0011] 본 발명의 실시예에 따른 익명 인증 서비스 방법은, 익명 ID 확인 장치로부터 서비스 제공 장치의 전역 연결키(Global Link Key)를 수신하는 과정과, 상기 서비스 제공 장치로부터 서비스 단말의 서명정보 또는 지역 가상 인덱스를 수신하는 과정과, 수신되는 상기 전역 연결키를 통해 상기 서명정보의 전역 가상 인덱스를 획득하여 상기 서비스 단말의 전역 연결성 정보를 확보하는 과정을 포함할 수 있다.

[0012] 여기서, 상기 전역 연결키를 수신하는 과정은, 상기 서비스 단말이 인명 인증 장치와 상호 협력하여 상기 서비스 단말의 사용자의 서명 비밀키를 획득하는 과정과, 상기 서비스 제공 장치가 상기 익명 ID 확인 장치와 상호 협력하여 상기 서비스 제공 장치의 공개키 및 비밀키쌍을 획득하는 과정과, 상기 서비스 제공 장치의 상위에서 전역 연결정보를 관리하고자 하는 전역 연결 장치가 상기 익명 ID 확인 장치와 상호 협력하여 상기 서비스 제공 장치의 상기 전역 연결키를 제공받는 과정을 포함할 수 있다.

[0013] 또한, 상기 지역 가상 인덱스를 수신하는 과정은, 상기 서비스 단말이 상기 서비스 제공 장치로부터 상기 공개키를 제공받고, 상기 공개키와 상기 서명 비밀키를 기반으로 하여 상기 서비스 단말의 사용자 서명을 생성하는 그룹서명 생성 과정과, 상기 서비스 제공 장치가 상기 사용자 서명의 유효 여부를 검증하는 그룹서명 검증 과정과, 상기 익명 ID 확인 장치가 상기 사용자 서명으로부터 익명ID를 계산한 후, 상기 익명 인증 장치와 상호 협력하여 상기 익명ID를 가지는 서비스 이용자를 확인하는 서명자 확인 과정과, 상기 서비스 제공 장치가 상기 공개키를 통해 상기 사용자 서명의 정당성 여부를 확인하고, 상기 비밀키를 통해 상기 사용자 서명으로부터 상기 서비스 단말의 가상 인덱스를 획득하여 상기 서비스 단말의 지역 연결성을 확보하는 지역연결 과정을 포함할 수 있다.

[0014] 또한, 상기 전역 연결성 정보를 확보하는 과정은, 상기 전역 연결 장치가 상기 서비스 제공 장치로부터 상기 서비스 단말의 상기 지역 가상 인덱스 또는 서명정보를 제공받는 과정과, 상기 전역 연결 장치가 상기 전역 연결키를 통해 상기 전역 가상 인덱스를 획득하여 상기 서비스 단말의 전역 연결성 정보를 확보하는 전역 연결 과정을 포함할 수 있다.

[0015] 또한, 상기 서명 비밀키를 획득하는 과정은, 상기 서비스 단말이 상기 사용자의 개인키 소유 증명 정보와 신원확인정보를 상기 익명 인증 장치로 제공하는 과정과, 상기 익명 인증 장치가 상기 서비스 단말의 사용자에 대응되는 익명ID를 포함하는 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정과, 상기 서비스 단말의 사용자를 등록하는 과정과, 상기 서비스 단말이 상기 그룹 멤버키에 대응되는 상기 서명 비밀키를 생성하여 저장하는 과정을 포함할 수 있다.

[0016] 또한, 상기 그룹 멤버키는, $(\hat{A}_i, x_i, z_i)$ ($\hat{A}_i = (\hat{g}_1 \hat{g}_4^{z_i} \hat{g}_3^{y_i})^{1/(\gamma+x_i)} \in G_1$ 및 $y_i, x_i, z_i \in Z_p^*$ 및 바이리니어 그룹 G_1, G_2 및 $g_1 = \varphi(g_2)$ 및 동형함수 φ 및 $g_2 \in G_2 \setminus \{1_{G_2}\}$ 및 $g_3, g_4 \in G_1 \setminus \{1_{G_1}\}$ 및 $\gamma \in Z_p^*$ 및 해시함수 $H : \{0,1\}^* \rightarrow Z_p$ 로 표현되고, 상기 서명 비밀키는 $gsk[i] = (\hat{A}_i, x_i, z_i, y_i)$ 로 표현되며, 상기 개인키 소유 증명 정보는 $g_3 \in G_1$ 에 대해 y_i 를 소유하고 있다는 증명 정보인 것을 특징으로 할 수 있다.

[0017] 또한, 상기 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정은, 상기 서비스 단말의 사용자가 이미 등록되어 있는 경우, 상기 서비스 단말의 사용자에 대응되는 상기 그룹 멤버키를 갱신하여 상기 서비스 단말로 제공하는 과정과, 상기 서비스 단말의 사용자가 미등록되어 있는 경우, 상기 서비스 단말의 사용자에 대응되는 상기 그룹 멤버키를 생성하여 상기 서비스 단말로 제공하는 과정과, 상기 서비스 단말의 사용자를 등록하는 과정을 포함할 수 있다.

[0018] 또한, 상기 등록하는 과정은, 상기 서비스 제공 장치가 서비스 제공자의 신원확인정보를 상기 익명 ID 확인 장치로 제공하는 과정과, 상기 익명 ID 확인 장치가 상기 서비스 제공자에 대응되는 상기 공개키 및 비밀키쌍과 추적키를 생성하여 상기 서비스 제공자를 등록하고, 상기 공개키 및 비밀키쌍을 상기 서비스 제공 장치로 제공하는 과정과, 상기 서비스 제공 장치가 상기 공개키 및 비밀키쌍으로부터 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정을 포함할 수 있다.

[0019] 또한, 상기 공개키는, (h_j, m_j, u_j, v_j) ($h_j = m_j^{\gamma}$, $u_j = m_j^{\xi_{1j}}$, $v_j = m_j^{\xi_{2j}} \in G_1$, $m_j \in G_1 \setminus \{1_{G_1}\}$, $\gamma_j, \xi_{1j}, \xi_{2j} \in Z_p^*$,

$H:\{0,1\}^{*}\rightarrow Z_{p}$, H는 해쉬함수, G_1 은 바이리니어 그룹)으로 표현되고, 상기 SP 공개키는 $gpk_{SP}[j]=(e,G_1,G_2,\hat{g}_1,\hat{g}_2,\hat{g}_3,\hat{g}_4,\hat{w},h_j,m_j,u_j,v_j)$ (e 는 동형함수, G_2 는 바이리니어 그룹, $g_1=\varphi(g_2)$, $g_2\in G_2\setminus\{1_{G_2}\}$, $g_3,g_4,h\in G_1\setminus\{1_{G_1}\}$, $w=g_2^{\gamma}\in G_2$, $\gamma\in Z_p^{*}$)으로 표현되며, 상기 비밀키는 (M_j,U_j,V_j) ($M_j\in G_2\setminus\{1_{G_1}\}$, $U_j=M_j^{\xi_{1j}}$, $V_j=M_j^{\xi_{2j}}\in G_2$)으로 표현되고, 상기 추격키는 ($tk_{sp}[j]=(\xi_{1j},\xi_{2j},\chi_j)$)($\chi_j,\xi_{1j},\xi_{2j}\in Z_p^{*}$)으로 표현되는 것을 특징할 수 있다.

[0020] 또한, 상기 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정은, 상기 서비스 제공 장치가 현재 세션의 그룹 공개 파라메터를 이용하여 상기 공개키로부터 상기 SP 공개키를 생성하고 저장하는 과정과, 상기 서비스 제공 장치가 상기 비밀키를 상기 LL 비밀키로 저장하는 과정을 포함할 수 있다.

[0021] 또한, 상기 그룹 공개 파라메터는 ($gpk=(e,G_1,G_2,g_1,g_2,g_3,g_4,w)$)로 표현되며, 상기 SP 공개키는 ($gpk_{SP}[j]=(e,G_1,G_2,\hat{g}_1,\hat{g}_2,\hat{g}_3,\hat{g}_4,\hat{w},h_j,m_j,u_j,v_j)$)로 표현되는 것을 특징으로 할 수 있다.

[0022] 또한, 상기 SP 공개키 및 LL 비밀키를 생성 및 저장하는 과정은, 상기 SP 공개키를 생성하고 저장하는 과정과 상기 LL 비밀키로 저장하는 과정을 수행하기 전에, 상기 서비스 제공 장치가 공개키 및 비밀키쌍이 $e(m_j,M_j)=e(u_j,U_j)=e(v_j,V_j)$ 의 식을 만족하는지를 확인하는 과정을 더 포함할 수 있다.

[0023] 또한, 상기 전역 연결키를 수신하는 과정은, 상기 전역 연결 장치가 전역 연결자의 신원확인정보를 상기 익명 ID 확인 장치에 제공하는 과정과, 상기 익명 ID 확인 장치가 상기 전역 연결자를 등록하는 과정과, 하위 서비스 제공 장치의 상기 전역 연결키를 상위 서비스 제공 장치로 제공하는 과정을 포함할 수 있다.

[0024] 또한, 상기 상위 서비스 제공 장치는 상기 전역 연결 장치이며, 상기 하위 서비스 제공 장치는 다수의 서비스 제공 장치들을 포함할 수 있다.

[0025] 또한, 상기 전역 연결키는, 상기 하위 서비스 제공 장치에 대하여 수학식 $LK_j=rb_j^{-1}$ (하위 서비스 제공 장치 j의 경우)로 표현될 수 있다.

[0026] 또한, 상기 전역 연결 장치는, 상기 수학식 $LK_j=rb_j^{-1}$ 을 통해 상기 전역 가상 인덱스를 제공받을 수 있다.

[0027] 또한, 상기 전역 연결키는, 상기 하위 서비스 제공 장치에 대하여 수학식 $(U_j=M^{\xi_{1j}},V_j=M^{\xi_{2j}},M)$ (서비스 제공 장치 j의 경우)로 표현될 수 있다.

[0028] 또한, 상기 전역 연결 장치는, 상기 수학식 $(U_j=M^{\xi_{1j}},V_j=M^{\xi_{2j}},M)$ 을 통해 상기 서명정보를 제공받을 수 있다.

[0029] 또한, 상기 그룹서명 생성 과정은, 상기 서비스 단말이 상기 서비스 제공 장치로부터 서비스 제공자의 SP 공개키를 획득하는 과정과, 상기 서비스 단말이 상기 SP 공개키 및 상기 서명 비밀키 및 메시지를 이용하여 상기 사용자 서명을 생성하는 과정을 포함할 수 있다.

[0030] 또한, 상기 서명자 확인 과정은, 상기 익명 ID 확인 장치가 상기 추적키를 이용하여 상기 사용자 서명으로부터 상기 서비스 이용자의 익명 ID를 추출하는 과정과, 상기 익명 ID 확인 장치가 상기 익명 인증 장치와 상호 협력하여 상기 익명ID에 대응되는 신원확인정보 및 상기 그룹 멤버키를 갖는 서비스 이용자를 확인하는 과정을 포함할 수 있다.

발명의 효과

[0031] 본 발명에 따른 계층적 연결성을 제공하는 익명 서비스 방법은, Short Group Signature에 기반한 익명 인증 동작을 수행하되, 지역 연결성과 전역 연결성을 포함하는 계층적 연결성이라는 개념을 도입하여 동일한 서비스 도메인 내에서의 연결성을 확보하는 동시에, 다수의 도메인을 포괄하는 상위 도메인의 전역연결성을 보장

할 수 있다. 즉, 본 발명에서는 각 서비스 제공자의 동일도메인 내부에서는 서비스 이용자 별로 고정된 값을 가지는 가상인덱스를 계산하되, 서비스 제공자들이 공모를 하여도 이와 동일한 값을 가지는 가상 인덱스를 계산할 수 없도록 하고, 다만, 상위에 전역 연결자를 두어 전역 도메인에서 서비스 이용자별로 고정된 값을 가지는 전역 인덱스를 계산하여 전역연결성을 확보할 수 있도록 해준다. 이에 따라 본 발명의 계층적 연결성을 제공하는 익명 서비스 방법은, 서비스 이용자의 익명성과 각 서비스제공 도메인 내에서만 유효한 지역 연결성을 유지하면서도, 다수의 서비스 제공 도메인을 포괄하는 전역 도메인에서 연결성을 제공할 수 있게 하여, 익명 지불 서비스 등 확장된 서비스를 제공할 수 있도록 해준다.

도면의 간단한 설명

[0032] 도 1은 본 발명의 실시예에 따른 익명 인증 서비스 방법을 구현하기 위한 익명 인증 서비스 장치에 대한 개략적인 구성 블록도,

도 2는 본 발명의 실시예에 따른 계층적 연결성을 제공하는 익명 인증 서비스 방법을 예시한 흐름도,

도 3은 도 2의 초기화 과정을 보다 구체적으로 설명하기 위한 도면,

도 4는 도 2의 서비스 이용자 가입 과정을 보다 구체적으로 설명하기 위한 도면,

도 5는 도 2의 서비스 제공자 가입 과정을 보다 구체적으로 설명하기 위한 도면,

도 6은 본 발명의 실시예에 따라 도 2의 전역 연결자 가입 과정을 구체적으로 설명하기 위한 도면,

도 7은 도 2의 그룹서명 생성 과정을 보다 구체적으로 설명하기 위한 도면,

도 8은 도 2의 지연 연결 과정을 보다 구체적으로 설명하기 위한 도면,

도 9는 본 발명의 실시예에 따라 도 2의 계층적 연결성을 위한 전역 연결 과정을 보다 구체적으로 설명하기 위한 도면.

발명을 실시하기 위한 구체적인 내용

[0033] 본 발명의 이점 및 특징, 그리고 그것들을 달성하는 방법은 첨부되는 도면과 함께 상세하게 후술되어 있는 실시예들을 참조하면 명확해질 것이다. 그러나 본 발명은 이하에서 개시되는 실시예들에 한정되는 것이 아니라 서로 다른 다양한 형태로 구현될 수 있으며, 단지 본 실시예들은 본 발명의 개시가 완전하도록 하고, 본 발명이 속하는 기술분야에서 통상의 지식을 가진 자에게 발명의 범주를 완전하게 알려주기 위해 제공되는 것이며, 본 발명은 청구항의 범주에 의해 정의될 뿐이다. 명세서 전체에 걸쳐 동일 도면부호는 동일 구성 요소를 지칭한다.

[0034] 본 발명의 실시예들을 설명함에 있어서 공지 기능 또는 구성에 대한 구체적인 설명이 본 발명의 요지를 불필요하게 흐릴 수 있다고 판단되는 경우에는 그 상세한 설명을 생략할 것이다. 그리고 후술되는 용어들은 본 발명의 실시예에서의 기능을 고려하여 정의된 용어들로서 이는 사용자, 운용자의 의도 또는 관례 등에 따라 달라질 수 있다. 그러므로 그 정의는 본 명세서 전반에 걸친 내용을 토대로 내려져야 할 것이다.

[0035] 첨부된 블록도의 각 블록과 흐름도의 각 단계의 조합들은 컴퓨터 프로그램 인스트럭션들에 의해 수행될 수도 있다. 이들 컴퓨터 프로그램 인스트럭션들은 범용 컴퓨터, 특수용 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서에 탑재될 수 있으므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비의 프로세서를 통해 수행되는 그 인스트럭션들이 블록도의 각 블록 또는 흐름도의 각 단계에서 설명된 기능들을 수행하는 수단을 생성하게 된다. 이들 컴퓨터 프로그램 인스트럭션들은 특정 방식으로 기능을 구현하기 위해 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 지향할 수 있는 컴퓨터 이용 가능 또는 컴퓨터 판독 가능 메모리에 저장되는 것도 가능하므로, 그 컴퓨터 이용가능 또는 컴퓨터 판독 가능 메모리에 저장된 인스트럭션들은 블록도의 각 블록 또는 흐름도 각 단계에서 설명된 기능을 수행하는 인스트럭션 수단을 내포하는 제조 품목을 생산하는 것도 가능하다. 컴퓨터 프로그램 인스트럭션들은 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에 탑재되는 것도 가능하므로, 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비 상에서 일련의 동작 단계들이 수행되어 컴퓨터로 실행되는 프로세스를 생성해서 컴퓨터 또는 기타 프로그램 가능한 데이터 프로세싱 장비를 수행하는 인스트럭션들은 블록도의 각 블록 및 흐름도의 각 단계에서 설명된 기능들을 실행하기 위한 단계들을 제공하는 것도 가능하다.

[0036] 또한, 각 블록 또는 각 단계는 특정된 논리적 기능(들)을 실행하기 위한 하나 이상의 실행 가능한 인스트럭션들을 포함하는 모듈, 세그먼트 또는 코드의 일부를 나타낼 수 있다. 또한, 몇 가지 대체 실시예들에서는 블록들 또는 단계들에서 언급된 기능들이 순서를 벗어나서 발생하는 것도 가능함을 주목해야 한다. 예컨대, 잇달아 도시되어 있는 두 개의 블록들 또는 단계들은 사실 실질적으로 동시에 수행되는 것도 가능하고 또는 그 블록들 또는 단계들이 때때로 해당하는 기능에 따라 역순으로 수행되는 것도 가능하다.

[0037] 본 발명의 익명 서비스 방법을 설명하기에 앞서 본 발명의 기반이 되는 Short Group Signature 에 대해 먼저 설명하기로 한다.

[0038] 그룹서명 기법은 D. Chaum 등이 1991년에 EUROCRYPT 컨퍼런스에서 처음 제안한 기법으로, 그룹에 속한 멤버는 누구라도 서명할 수 있으며 검증자는 서명의 옳고 그름을 검증할 수 있으나 서명자에 대해 어떤 정보도 알아낼 수 없도록 한다. 그룹 관리자는 그룹서명 기법에서 가장 중요한 존재로, 그룹서명을 추적하여 그룹서명자의 신원을 알아낼 수 있다.

[0039] Short Group Signature는 D. Boneh 등이 2004년에 CRYPTO 컨퍼런스에 제안한 그룹서명 기법으로, 서명의 길이가 고정적이고 짧으며(1553bits), 서명 및 검증 시간이 상대적으로 짧다는 장점을 가진다.

[0040] 이하, 본 발명의 실시예에 대해 첨부된 도면을 참조하여 상세히 설명하기로 한다.

[0041] 도 1은 본 발명의 실시예에 따른 익명 인증 서비스 방법을 구현하기 위한 익명 인증 서비스 장치의 구성 블록도로서, 서비스 단말(100), 익명 인증 장치(110), 서비스 제공 장치 그룹(120), 익명 ID 확인 장치(130), 전역 연결 장치(140) 등을 포함할 수 있다.

[0042] 도 1을 참조하면, 서비스 단말(100)은 익명 인증 장치(110)로부터 익명 인증 수단, 예를 들어 익명ID, 비밀키 등을 발급받아 서비스 제공 장치 그룹(120)으로부터 익명으로 서비스를 이용할 수 있도록 하는 역할을 할 수 있다. 본 발명의 실시예에 따른 서비스 단말(100)은 서비스 이용자에 의해 구동 및 이용되므로, 이하에서는 설명의 편의를 위해 서비스 이용자로 총칭하기로 한다.

[0043] 익명 인증 장치(110)는 서비스 이용자의 실명을 확인하여 익명 인증 수단을 발급하며, 문제가 있는 경우에는 익명 ID 확인 장치(130)와 함께 사용자의 실명을 추적할 수 있으나 단독으로는 추적이 불가능하다.

[0044] 서비스 제공 장치 그룹(120)은 하위 서비스 제공 장치 그룹으로서, 다수의 서비스 제공 장치들(120/1~120/n)을 포함할 수 있다. 서비스 제공 장치 그룹(120)에서 임의의 서비스 제공 장치, 예를 들어 서비스 제공 장치1(120/1)은 익명 ID 확인 장치(130)로부터 익명 ID를 확인하고 지역 연결성을 제공할 수 있다. 또한, 서비스 제공 장치1(120/1)은 서비스 단말(100)로부터 서명 전송 과정이 포함되는 익명 인증 인가 요청시에 서비스 단말(100)로 서비스를 제공할 수 있다.

[0045] 익명 ID 확인 장치(130)는 서비스 제공 장치1(120/1)로부터 익명인증 트랜잭션을 전달받아, 그로부터 익명 ID를 확인할 수 있다.

[0046] 본 발명의 실시예에 따른 전역 연결 장치(140)는 익명 ID 확인 장치(130)로부터 서비스 제공 장치 그룹(120)의 각각의 서비스 제공 장치에 대응하는 전역 연결키를 수신할 수 있으며, 서비스 제공 장치 그룹(120)으로부터 서비스 단말(100)의 서명정보 또는 지역 가상 인덱스를 수신하고, 전역 연결키를 통해 서명정보의 전역 가상 인덱스를 획득함으로써, 서비스 단말(140)의 전역 연결성 정보를 확보할 수 있다.

[0047] 본 발명에서는 지역 연결성이라는 개념과 또한 추가적으로 전역 연결자를 통한 계층적 연결성을 제안하고, 이에 따라 Short Group Signature을 이용한 익명 서비스 방법을 변형함으로써, Short Group Signature에 의한 익명성을 유지하되 동일한 서비스 도메인 내의 지역 연결성과 상위의 도메인에서 전역 연결성을 추가적으로 지원할 수 있도록 하는 새로운 익명 서비스 방법을 제안하고자 한다.

[0048] 지역 연결성이라는 개념은 익명성을 약간 완화시켜 마일리지 서비스 등 유용한 기능을 제공하기 위해 제안된 것으로, 특히 이용자의 반복적인 가입과 탈퇴 하에서도 연속적으로 부분 연결성을 제공하도록 설계하여 멤버쉽의 변화와 상관없이 안정적인 마일리지 서비스 등의 유용한 기능을 제공할 수 있도록 하기 위한 것이다.

[0049] 다만, 본 발명의 익명 서비스 방법을 사용하는 서비스 제공 장치는 동일 도메인 내에서의 그룹서명은 연결할 수 있지만(즉, 동일서명자가 생성한 서명을 확인할 수 있지만), 그룹 서명자의 익명ID를 확인하거나 서비스 도메인간의 “지역연결성” 정보를 공유할 수 는 없다.

[0050] 전역 연결성 개념은 지불 서비스 등 기존의 서비스 도메인보다 포괄적인 범위에서 서비스 이용자를 연결할 필요가 있을 때 유용하게 사용될 수 있는 개념으로, 지역 연결성을 제공받는 각각의 도메인을 포괄하는 상위의 도메인에서 서비스 이용자들을 전역적으로 연결할 수 있는 전역 연결 장치를 도입한다.

[0051] 도 2는 본 발명의 실시예에 따른 지역 연결성을 제공하는 익명 인증 서비스 방법을 도시한 도면이다.

[0052] 도 2을 참조하면, 상기 익명 인증 서비스 방법은 초기화(SetUp) 과정(S200), 서비스 이용자 가입(Join) 과정(S202), 서비스 제공자 가입 과정(S204), 전역 연결자 가입 과정(S206), 그룹서명 생성(Sign) 과정(S208), 그룹서명 검증(Verify) 과정(S210), 서비스 이용자 추적 과정(S212), 익명 ID 확인(Open) 과정(S214), 지역 연결(Local-Link) 과정(S216), 지역 가상 인덱스 또는 서명정보 수신 과정(S218), 전역 가상 인덱스 획득 과정(S220), 전역 연결 과정(S22) 등을 포함할 수 있다.

[0053] 이하에서, 각 과정을 보다 구체적으로 살펴보면 다음과 같다.

[0054] 먼저 초기화(SetUp) 과정(S100)에서는 도 3에 도시된 바와 같이, 익명 인증 장치(110)가 다음과 같은 과정을 수행한다.

[0055] 단계 S200-1, 익명 인증 장치(110)는 보안 파라미터 K를 입력으로 받아서 다음을 수행한다. 먼저 바이리니어(bilinear) 그룹쌍 (G_1, G_2) 와 결합된 계산 가능한 동형함수 φ 와 바이리니어 함수 $e: G_1 \times G_2 \to G_T$, 그리고 해쉬 함수 $H: \{0,1\}^* \to \mathbb{Z}_p$ 를 생성한다. 그리고 임의의 생성원 $g_2 \in G_2 \setminus \{1_{G_2}\}$ 와 $g_3, g_4, h \in G_1 \setminus \{1_{G_1}\}$ 을 선택하고 $g_1 = \varphi(g_2)$ 을 계산하며, 마스터 비밀키 $\gamma \in \mathbb{Z}_p^*$ 를 선택하고 그룹 공개키 $w = g_2^{\gamma} \in G_2$ 를 계산하여, 그룹 공개파라미터 $gpk = (e, G_1, G_2, g_1, g_2, g_3, g_4, w)$ 를 획득한다.

[0056] 단계 S200-2, 익명 인증 장치(110)는 그룹 공개파라미터 gpk 를 모든 참가자에게 공개한다. 이때, 그룹 공개파라미터는 철폐(Revocation) 이벤트가 발생할 때마다 갱신된다. 또한 선택적으로, 그룹 공개 파라미터에 페어링 함수 계산을 줄이기 위한 $\eta_1 \leftarrow e(g_1, g_2)$, $\eta_4 \leftarrow e(g_3, g_2)$, $\eta_5 \leftarrow e(g_4, g_2)$ 을 공개키에 포함할 수 있다.

[0057] 서비스 이용자 가입 과정(S202)은 그룹에 가입하여 그룹 서명키를 사용하려는 서비스 이용자(100)를 위한 절차이며, 서비스 제공자 가입 과정(S204)은 지역 연결성을 확보하기 위한 서비스제공서버를 위한 절차이다. 또한, 전역 연결자 가입 과정(S206)은 다수의 특정한 이미 가입된 서비스제공자에 대하여 전역적인 연결정보를 관리할 수 있는 전역 연결 장치(140)를 위한 절차이다.

[0058] 도 4에 도시된 바와 같이, 서비스 이용자 가입 과정(S204)은 서비스 이용자(100)와 익명 인증 장치(110)에 의해 수행되며, 이때 서비스 이용자(100)와 익명 인증 장치(110)사이에는 보안채널이 형성되어 있다고 가정한다.

[0059] S202-1에서, 서비스 이용자(100)는 임의의 난수 $y_i \in \mathbb{Z}_p^*$ 를 선택하고 $g_3^{-y_i} \in G_1$ 을 계산한다. 그리고 이에 대한 개인키 소유 증명(Proof of Possession, POP), 즉, 생성원 y_i 를 소유하고 있다는 증명 정보, $POP(y_i)$ 를 생성한 후, 익명 인증 장치(110)에 (신원확인정보, $POP(y_i)$)을 송신한다.

[0060] S202-2에서, 익명 인증 장치(110)는 가입하려는 서비스 이용자(100)로부터 전송되는 (신원확인정보, $POP(y_i)$)를 수신하여 이의 유효성을 확인한 후, 서비스 이용자(100)의 재가입 여부를 확인한다.

[0061] S202-3에서, 서비스 이용자(100)가 이미 가입되어 (신원확인정보, $POP(y_i)$)이 이용자 목록(User-List)에 존재하면, 익명 인증 장치(110)는 임의의 난수 $x^i \in \mathbf{Z}_p^*$ 를 선택하고 익명ID인 $\hat{A}_i = (\hat{g}_1 \hat{g}_4^{-z_i} \hat{g}_3^{-y_i})^{1/(y_i+x_i)} \in G_1$ 를 계산한다. 그리고 서비스 이용자(100)에 대한 그룹멤버키 $(\hat{A}_i, x_i, z_i)$ 을 생성하여, 해당 서비스 이용자(100)에게 송신한다.

[0062] S202-4에서, 서비스 이용자(100)가 최초로 가입하여 (신원확인정보, $POP(y_i)$)이 이용자 목록에 없으면, 익명 인증 장치(110)는 서비스 이용자(100)에 대한 그룹멤버키 $(\hat{A}_i, x_i, z_i)$ 를 서비스 이용자(100)에 송신하면서, (신원확인정보, $POP(y_i)$)을 이용자 목록(User-List)에 추가하여 해당 서비스 이용자(100)를 등록한다.

[0063] S202-5에서, 서비스 이용자(100)는 $(\hat{A}_i, x_i, z_i)$ 를 수신한 후, 이하의 [수학식 1]이 성립하는지 확인한 후, 수학식4가 성립되면 서비스 이용자(100)는 $gsk[i] = (\hat{A}_i, x_i, z_i, y_i)$ 을 자신의 그룹서명 비밀키로 저장한다.

수학식 1

[0064] $$e(\hat{A}_i, \hat{w} \cdot \hat{g}_2^{x_i}) = e(\hat{g}_1 \hat{g}_4^{-z_i} \hat{g}_3^{-y_i}, \hat{g}_2) \quad (= \hat{\eta}_1 \cdot \hat{\eta}_5^{-z_i} \cdot \hat{\eta}_4^{-y_i}) .$$

[0065] 도 5에 도시된 바와 같이, 서비스 제공자 가입 과정(S204)은 임의의 서비스 제공 장치, 예를 들어 서비스 제공 장치1(120/1)과 익명 ID 확인 장치(130)에 의해 수행되며, 이때 서비스 제공 장치1(120/1)과 익명 ID 확인 장치(130) 사이에는 보안채널이 형성되어 있다고 가정한다.

[0066] S204-1에서, 서비스 제공 장치1(120/1)은 자신의 SP 신원확인정보를 익명 ID 확인 장치(130)에 송신한다.

[0067] S204-2에서, 익명 ID 확인 장치(130)는 서비스 제공 장치1(120/1)로부터 전송되는 SP 신원확인정보를 수신하여 이의 유효성을 확인한 후, 임의의 생성원 $m_j \in G_1 \setminus \{1_{G_1}\}$, $M_j \in G_2 \setminus \{1_{G_1}\}$ 와 임의의 난수 $\chi_j, \xi_{1j}, \xi_{2j} \in \mathbf{Z}_p^*$ 를 선택하고 $h_j = m_j^{\chi_j}$, $u_j = m_j^{\xi_{1j}}, v_j = m_j^{\xi_{2j}} \in G_1$, $U_j = M_j^{\xi_{1j}}, V_j = M_j^{\xi_{2j}} \in G_2$ 를 계산한다. 그리고 공개키 및 비밀키쌍 $(h_j, m_j, u_j, v_j, M_j, U_j, V_j)$ 과 추적키 $tk_{sp}[i] = (\xi^{1i}, \xi^{2i}, \chi^i)$ 를 획득한 후, 공개키 및 비밀키쌍 $(h_j, m_j, u_j, v_j, M_j, U_j, V_j)$ 은 서비스 제공 장치1(120/1)에게 송신한다.

[0068] S204-2에서, 익명 ID 확인 장치(130)는 ($(h_j, m_j, u_j, v_j, M_j, U_j, V_j)$, SP신원확인정보, $(\chi_j, \xi_{1j}, \xi_{2j})$)을 서비스 제공 장치 목록(SP-List)에 추가하여, 서비스 제공 장치1(120/1)을 등록한다.

[0069] S204-3에서, 서비스 제공 장치1(120/1)은 공개키 및 비밀키쌍 $(h_j, m_j, u_j, v_j, M_j, U_j, V_j)$ 를 수신한 후 이하의 [수학식 2]가 성립하는지 확인한다. 만약 [수학식 2]가 성립되면, 서비스 제공 장치1(120/1)은 $LLK_{SP}[j] = (M_j, U_j, V_j)$ 을 자신의 LL 비밀 키로 저장하고, 현 세션에 대응하는 공개 파라미터 $gpk = (e, G_1, G_2, g_1, g_2, g_3, g_4, w)$ 를 이용하여 SP공개키 $gpk_{SP}[j] = (e, G_1, G_2, \hat{g}_1, \hat{g}_2, \hat{g}_3, \hat{g}_4, \hat{w}, h_j, m_j, u_j, v_j)$ 를 생성하여 공개한다.

수학식 2

[0070] $$e(m_j, M_j) = e(u_j, U_j) = e(v_j, V_j)$$

[0071] 이때, 서비스 이용자(100)는 SP 공개키에 포함된 값들이 익명 ID 확인 장치(130)가 서비스 제공 장치1(120/1)을 위해 발급한 값임을 검증할 수 있다고 가정하며, SP공개키는 철폐 이벤트가 발생할 때마다 갱신된다. 또한 페어링 함수 계산량을 줄이기 위해 $\hat{\eta}_1 \leftarrow e(\hat{g}_1, \hat{g}_2)$, $\hat{\eta}_4 \leftarrow e(\hat{g}_3, \hat{g}_2)$, $\hat{\eta}_5 \leftarrow e(\hat{g}_4, \hat{g}_2)$, $\tilde{\eta}_2 \leftarrow e(h_j, \hat{g}_2)$, $\tilde{\eta}_3 \leftarrow e(h_j, \hat{w})$, $\tilde{\eta}_5 \leftarrow e(m_j, \hat{g}_2)$, $\tilde{\eta}_6 \leftarrow e(m_j, \hat{w})$ 을 공개 파라미터에 포함할 수 있다.

[0072] 도 6은 본 발명의 실시예에 따른 전역 연결자 가입 과정(S206)을 구체적으로 설명하기 위한 도면이다.

[0073] 도 6에 도시된 바와 같이, 전역 연결자 가입 과정(S206)은 전역 연결 장치(140)와 익명 ID 확인 장치(130)에 의해 수행되며, 이때 전역 연결 장치(140)와 익명 ID 확인 장치(130) 사이에는 보안채널이 형성되어 있다고 가정한다.

[0074] 전역 연결 장치(140)는 자신의 전역 연결자 신원확인정보를 익명 ID 확인 장치(130)로 송신할 수 있다(S206-1).

[0075] 익명 ID 확인 서버(130)는 전역 연결 장치(140)로부터 전송되는 전역 연결자 신원확인정보를 수신하여 이의 유효성을 확인할 수 있다(S206-2).

[0076] 이후, 익명 ID 확인 장치(130)는 해당하는 전역 연결자에 포함될 하위 도메인의 서비스 제공자 각각에 대응하는 전역 연결키를 전역 연결 장치(140)로 전송할 수 있다(S206-3).

[0077] 이때, 전역 연결자에 포함될 하위 서비스제공자의 목록을 전역 연결 장치(140)의 요청, 자격 등 정책에 따라 선택적으로 선정하도록 할 수 있다.

[0078] 또한, 전역 연결키는 방법1에서 $LK_j = rb_j^{-1}$ (하위 서비스제공자 j 의 경우)으로 표현되고, 방법 2에서 $(U_j = M^{b_{1,j}}, V_j = M^{b_{2,j}^{-1}}, M)$ (서비스제공자 j 의 경우)로 표현될 수 있다.

[0079] 그룹서명 생성(Sign) 과정(S208)에서는, 서비스 이용자(100)는 도 7에 도시된 바와 같이 상호 협력하여 그룹서명을 생성한다.

[0080] S208-1에서, 서비스 이용자(100)는 서비스 제공 장치1(120/1)로부터 SP 공개키 $gpk_{SP}[j]$ 를 획득한다.

[0081] S208-2에서, 서비스 이용자(100)는 SP 공개키 $gpk_{SP}[j]$, 비밀키 $gsk[i] = (\hat{A}_i, x_i, z_i, y_i)$, 메시지 M 를 이용하여 그룹서명을 생성한다.

[0082] 즉, 임의의 난수 $\alpha, \beta \in Z_p$ 를 선택한 후, $T_1 = u_j^{\alpha}$, $T_2 = v_j^{\beta}$, $T_3 = \hat{A}_i h_j^{\alpha+\beta}$, $T_4 = g_1^{-s} m_j^{\alpha-\beta}$ 를 계산하고, $\delta_1 = x_i \alpha$ 와 $\delta_2 = x_i \beta$ 를 계산한다. 그리고, 임의의 난수 $r_\alpha, r_\beta, r_x, r_y, r_z, r_{\delta_1}, r_{\delta_2} \in Z_p$ 을 선택하고 다음 [수학식 3]과 같이 R_1, R_2, R_3, R_4, R_5, R_6 을 계산한다. 계산된 값들과 메시지 M 을 이용하여 해쉬 값 $c = H(M, T_1, T_2, T_3, R_1, R_2, R_3, R_4, R_5, R_6)$ 를 계산한 후, $s_\alpha = r_\alpha + c\alpha$, $s_\beta = r_\beta + c\beta$, $s_{x_i} = r_{x_i} + cx_i$, $s_{z_i} = r_{x_i} + cz_i$, $s_{y_i} = r_{y_i} + cy_i$, $s_{\delta_1} = r_{\delta_1} + c\delta_1$, $s_{\delta_2} = r_{\delta_2} + c\delta_2$ 을 계산하여, 그룹서명 $\sigma = (T_1, T_2, T_3, T_4, c, s_\alpha, s_\beta, s_x, s_y, s_z, s_{\delta_1}, s_{\delta_2})$ 를 생성 및 출력한다.

수학식 3

$$R_1 \leftarrow u_j^{r_\alpha}, \quad R_2 \leftarrow v_j^{r_\beta},$$

$$R_3 \leftarrow e(T_3, \hat{g}_2)^{r_{x_i}} \cdot e(h_j, \hat{w})^{-r_\alpha - r_\beta} \cdot e(h_j, \hat{g}_2)^{-r_{\delta_1} - r_{\delta_2}} \cdot e(\hat{g}_3, \hat{g}_2)^{r_{y_i}} \cdot e(\hat{g}_4, \hat{g}_2)^{r_{z_i}},$$

$$R_4 \leftarrow g_1^{r_{z_i}} \cdot m_j^{-r_\alpha + r_\beta}, \quad R_5 \leftarrow T_1^{r_{x_i}} u_j^{-r_{\delta_1}}, \quad R_6 \leftarrow T_2^{r_{x_i}} v_j^{-r_{\delta_2}}.$$

[0083]

[0084] 그룹서명 검증(Verify) 과정(S210)에서는, 서비스 제공 장치1(120/1) 또는 임의의 참가자는 SP 공개키 $gpk_{SP}[j]$, 메시지 M, 서명 $\tilde{\sigma} = (\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4, \tilde{c}, \tilde{s}_\alpha, \tilde{s}_\beta, \tilde{s}_{x_i}, \tilde{s}_{y_i}, \tilde{s}_{z_i}, \tilde{s}_{\delta_1}, \tilde{s}_{\delta_2})$ 에 대해서 다음을 수행한다.

[0085] 서비스 제공 장치1(120/1) 또는 임의의 참가자는 이하의 [수학식 4]에 따라 $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$, $\tilde{R}_4$, $\tilde{R}_5$, $\tilde{R}_6$ 를 계산하고, 계산된 $\tilde{R}_1$, $\tilde{R}_2$, $\tilde{R}_3$, $\tilde{R}_4$, $\tilde{R}_5$, $\tilde{R}_6$ 과 서명에 포함된 $\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4$, 메시지 M 을 이용하여 해쉬 값 $H(M, \tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4, \tilde{R}_1, \tilde{R}_2, \tilde{R}_3, \tilde{R}_4, \tilde{R}_5, \tilde{R}_6)$ 를 생성하고 이 값이 그룹서명에 포함된 $\tilde{c}$ 와 같은지 확인한다. 만약 두 값이 같다면 1(그룹서명 유효)을 출력하고 그렇지 않다면 0(그룹서명 미유효)을 출력한다.

수학식 4

$$\tilde{R}_1 \leftarrow u_j^{\tilde{s}_\alpha} \cdot \tilde{T}_1^{-\tilde{c}}, \quad \tilde{R}_2 \leftarrow v_j^{\tilde{s}_\beta} \cdot \tilde{T}_2^{-\tilde{c}},$$

$$\tilde{R}_3 \leftarrow e(\tilde{T}_3, \hat{g}_2)^{\tilde{s}_x} \cdot e(h_j, \hat{w})^{-\tilde{s}_\alpha - \tilde{s}_\beta} \cdot e(h_j, \hat{g}_2)^{-\tilde{s}_{\delta_1} - \tilde{s}_{\delta_2}} \cdot e(\hat{g}_3, \hat{g}_2)^{\tilde{s}_{y_i}} \cdot e(g_4, \hat{g}_2)^{\tilde{s}_{z_i}} \cdot \left(\frac{e(\tilde{T}_3, \hat{w})}{e(\hat{g}_1, \hat{g}_2)} \right)^{\tilde{c}}$$

$$\tilde{R}_4 \leftarrow \tilde{T}_4^{\tilde{c}} \cdot m_j^{-\tilde{s}_\alpha + \tilde{s}_\beta} g_1^{\tilde{s}_{z_i}},$$

$$\tilde{R}_5 \leftarrow \tilde{T}_1^{-\tilde{s}_x} \cdot u_j^{-\tilde{s}_{\delta_1}}, \quad \tilde{R}_6 \leftarrow \tilde{T}_2^{\tilde{s}_x} \cdot v_j^{-\tilde{s}_{\delta_2}}.$$

[0086]

[0087] 서명자 확인(Open) 과정은 서비스 이용자 추적 과정(S212)과 익명 ID 확인 과정(S214)을 포함할 수 있으며, 이들 과정에서는, 익명 ID 확인 장치(130)와 익명 인증 장치(110)가 다음의 과정들을 수행한다.

[0088] 익명 ID 확인 장치(130)는 서비스 제공 장치1(120/1) 또는 임의의 참가자로부터 제공되는 SP 공개키 $gpk_{SP}[j]$ 와 이에 대응하는 추적키 $tk_{sp}[j] = (\xi_{1j}, \xi_{2j}, \chi_j)$, 그리고 메시지 M 과 이에 대응하는 그룹 서명 $\tilde{\sigma} = (\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4, \tilde{c}, \tilde{s}_\alpha, \tilde{s}_\beta, \tilde{s}_{x_i}, \tilde{s}_{y_i}, \tilde{s}_{z_i}, \tilde{s}_{\delta_1}, \tilde{s}_{\delta_2})$ 에 대하여 다음을 수행한다.

[0089] 먼저, 그룹서명의 정당성을 확인한 후, $tk_{sp}[j] = (\xi_{1j}, \xi_{2j}, \chi_j)$ 을 이용하여 $A_i = g_1^{-x} = \tilde{T}_4 \cdot (\tilde{T}_1^{-\xi_{1j}} \tilde{T}_2^{-\xi_{2j}})$ 을 계산한다. 이때, 서명에 포함된 세 가지 $\tilde{T}_1 \leftarrow u_j^{r_\alpha}$, $\tilde{T}_2 \leftarrow v_j^{r_\beta}$, $\tilde{T}_3 \leftarrow \hat{A}_i h_j^{\alpha+\beta}$ 과 추적키 $tk_{sp}[j] = (\xi_{1j}, \xi_{2j}, \chi_j)$ 를 이용하여 갱신된 익명ID 정보 값 $\hat{A}_i = \tilde{T}_3 \cdot (\tilde{T}_1^{-\chi\xi_{1j}} \tilde{T}_2^{-\chi\xi_{2j}})$ 도 복호화할 수 있다.

[0090] 그리고 익명 인증 장치(110)와 익명 ID 확인 장치(130)는 상호 협력하여 (필요한 경우, 익명 인증 장치(110)의 이용자 목록(User-List)에서 익명ID에 대응되는 신원확인정보 및 상기 그룹 멤버키를 가지는 서비스 이용

자를 비교 검색하여) 익명ID에 대응되는 사용자를 확인한다.

[0091] 지역연결(Local-Link) 과정(S216)에서는, 서비스 제공 장치1(120/1)은 도 8에 도시된 바와 같이 동작하여 동일 서비스 도메인내에서의 연결성을 확보한다.

[0092] S216-1에서, 서비스 제공 장치1(120/1)은 SP 공개키와 자신의 비밀 LL 키 $LLK_{SP}[j] = (M_j, U_j, V_j)$, 그리고 메시지 M 과 이에 대응하는 그룹 서명 $\tilde{\sigma} = (\tilde{T}_1, \tilde{T}_2, \tilde{T}_3, \tilde{T}_4, \tilde{c}, \tilde{s}_\alpha, \tilde{s}_\beta, \tilde{s}_{x_j}, \tilde{s}_{y_j}, \tilde{s}_{z_j}, \tilde{s}_\delta, \tilde{s}_\varepsilon)$ 에 획득한 후, 그룹서명이 자신의 SP공개키에 대하여 정당한지 그룹서명 검증 알고리즘을 이용하여 확인한다. 만일 정당하다면, 이하의 [수학식 5]에 따라 자신의 비밀LL키를 이용하여 서비스 이용자(100)의 가상인덱스를 계산한다.

수학식 5

[0093] $$P \leftarrow e(\tilde{T}_4, M_j) \cdot e(\tilde{T}_1, U_j)^{-1} \cdot e(\tilde{T}_2, V_j)$$

[0094] S216-2에서, 서비스 제공 장치1(120/1)은 $P = e(A_j, M_j) = e(g_1^{-z_j}, M_j)$ 를 가상인덱스로 획득하고, 이를 익명토큰 목록(AT-List)에 추가하여 지역 연결성을 확보한다.

[0095] 이와 같이, 본 발명의 지역연결 과정(S216)에 따르면, 서비스 제공 장치1(120/1)는 익명 사용자의 익명ID에 해당하는 A_i 를 계산하지 못하나, 고정된 값을 가지는 가상인덱스 $P = e(A_j, M_j) = e(g_1^{-z_j}, M_j)$ 은 계산할 수 있게 된다.

[0096] 이에 서비스 제공 장치1(120/1)은 서비스 이용자의 실명 ID가 고정된 값을 가지는 가상인덱스를 이용하여 서비스 이용자를 구분하고 마일리지 서비스, 벌점 부여, 서비스 이용 기록 분석 등의 기능을 수행할 수 있게 된다.

[0097] 즉, 서비스 제공 장치1(120/1)는 익명을 유지하면서도 동일한 서비스 도메인 내에서의 연결성을 지원할 수 있게 된다.

[0098] 그럼에도 불구하고, 서비스제공자 j, k가 공모를 하여도 같은 사용자의 서명들로부터 동일한 가상인덱스를 계산할 수 없어, 서로 같은 사용자인지를 확인할 수 없게 된다.

[0099] 즉, 서비스제공자 j, k는 같은 사용자의 서명들로부터 각각 $P_j = e(A_j, M_j) = e(g_1^{-z_j}, M_j)$, $P_k = e(A_j, M_k) = e(g_1^{-z_j}, M_k)$ 만을 계산할 수 있어, 동일한 값의 가상인덱스를 획득하지 못하게 된다.

[0100] 따라서, 본 발명에서는 동일 서비스 도메인 내부에서만 연결성이 확보될 수 있을 뿐, 서로 다른 서비스 도메인간의 연결은 지원하지 않으므로, 지역 연결성(Local Linkability) 기능을 만족할 수 있게 된다.

[0101] 본 발명의 실시예에 따른 전역연결(Global-Link) 과정에서, 전역 연결 장치(140)는 도 9에 도시된 바와 같이 동작하여 전역 도메인 내에서의 연결성을 확보할 수 있다.

[0102] 방법1의 경우, 해당 전역 연결 장치(140)에 포함되는 서비스 제공 장치1(120/1)은 자신의 지역 가상인덱스 $e(T_4, M_j) \cdot e(T_1, U_j)^{-1} e(T_2, V_j) \rightarrow e(g_0^{-x_i}, M_j)$ 를 전역 연결 장치(140)로 제공할 수 있다(S218). 전역 연결 장치(140)는 자신이 포함하는 서비스 제공 장치 각각에 대하여 이미 확보하고 있는 전역 연결키(Global Link Key) $LK_j = rb_j^{-1}$ 를 이용하여 전역 가상 인덱스 $e(g_0^{-x_i}, M_j)^{LK_j} = e(g_0^{-x_i}, \mu^{b_j})^{rb_j^{-1}} \rightarrow e(g_0^{-x_i}, \mu^r)$ 를 계산해 낼 수 있다(S220).

[0103] 방법2의 경우, 전역 연결 장치(140)에 포함되는 서비스 제공 장치1(120/1)은 자신이 서비스 이용자로부터 받은 서명값을 전역 연결 장치(140)에 제공할 수 있다(S218). 전역 연결 장치(140)는 자신이 포함하는 서비스

제공 장치 각각에 대하여 이미 확보하고 있는 전역연결키(Global Link Key) $(U_j = M^{\phi_{1,j}}, V_j = M^{\phi_{2,j}}, M)$ 를 이용하여 전역 가상 인덱스 $e(T_4, M) \cdot e(T_1, U_j)^{-1} e(T_2, V_j) \rightarrow e(g_0^{-x_i}, M)$ 를 계산해 낼 수 있다(S220).

[0104] 이와 같이, 본 발명의 전역연결 과정에 따르면, 상위 서비스 제공 장치인 전역 연결 장치(140)는 익명 사용자의 익명ID에 해당하는 A_i 를 계산하지 못하나, 고정된 값을 가지는 전역 인덱스 $P = e(g_0^{-x_i}, \mu^r)$ (방법1), $P = e(g_1^{-x_i}, M^r)$ (방법2)을 계산할 수 있게 된다.

[0105] 이에, 상위 서비스 제공 장치인 전역 연결 장치(140)는 하위 서비스 제공 장치인 서비스 제공 장치 그룹(120)을 포괄하는 서비스 도메인에서 고정된 값을 갖는 전역 인덱스를 이용하여 서비스 이용자 지불정보, 금융정보 관리 수행 등의 서비스를 제공할 수 있게 된다.

[0106] 즉, 전역 연결 장치(140)는 하위의 서비스 제공 장치들의 입장에서는 서로 연결이 불가능한 서비스 이용자의 트랜잭션에 대해서 전역적인 연결성을 지원할 수 있게 된다. 서비스 제공 장치들은 j, k는 같은 사용자의 서명들로부터 각각 다른 지역 가상인덱스 $P_j = e(A_i, M_j) = e(g_1^{-x_i}, M_j)$, $P_k = e(A_i, M_k) = e(g_1^{-x_i}, M_k)$ 을 계산할 수 있고, 이들을 포함하는 전역 연결 장치(140)는 방법1의 경우, 이 값으로부터 각각 $e(g_0^{-x_i}, M_j)^{LK_j} = e(g_0^{-x_i}, \mu^{b_j})^{rb_j^{-1}} \rightarrow e(g_0^{-x_i}, \mu^r)$, $e(g_0^{-x_i}, M_k)^{LK_k} = e(g_0^{-x_i}, \mu^{b_k})^{rb_k^{-1}} \rightarrow e(g_0^{-x_i}, \mu^r)$ 을 계산하여 동일한 값을 얻게 되고, 방법 2의 경우, 서비스 제공 장치들은 j, k가 서비스 이용자로부터 받은 서명값으로부터 각각 $e(T_4, M) \cdot e(T_1, U_j)^{-1} e(T_2, V_j) \rightarrow e(g_0^{-x_i}, M)$, $e(T_4', M) \cdot e(T_1', U_k)^{-1} e(T_2', V_k) \rightarrow e(g_0^{-x_i}, M)$ 을 계산하여 역시 동일한 값을 얻게 된다.

[0107] 따라서, 본 발명의 실시예에서는 동일 서비스 도메인 내부에서만 연결성이 확보되는 동시에 상위의 전역연결성 역시 제공할 수 있는 계층적 연결성(Hierarchical Linkability) 기능을 만족할 수 있게 된다.

[0108] 이상 설명한 바와 같은 본 발명의 실시예에 의하면, 지역 연결성과 전역 연결성을 포함하는 계층적 연결성이라는 개념을 도입하여 동일한 서비스 도메인 내에서의 연결성을 확보하는 동시에, 다수의 도메인을 포괄하는 상위 도메인의 전역연결성을 보장할 수 있다. 즉, 본 발명에서는 각 서비스 제공자의 동일도메인 내부에서는 서비스 이용자 별로 고정된 값을 가지는 가상인덱스를 계산하되, 서비스 제공자들이 공모를 하여도 이와 동일한 값을 가지는 가상 인덱스를 계산할 수 없도록 하고, 다만, 상위에 전역 연결자를 두어 전역 도메인에서 서비스 이용자별로 고정된 값을 가지는 전역 인덱스를 계산하여 전역연결성을 확보할 수 있도록 해준다. 이에 따라 본 발명의 계층적 연결성을 제공하는 익명 서비스 방법은, 서비스 이용자의 익명성과 각 서비스제공 도메인 내에서만 유효한 지역 연결성을 유지하면서도, 다수의 서비스 제공 도메인을 포괄하는 전역 도메인에서 연결성을 제공할 수 있게 하여, 익명 지불 서비스 등 확장된 서비스를 제공할 수 있도록 해준다.

부호의 설명

[0109] 100: 서비스 단말

110: 익명 인증 장치

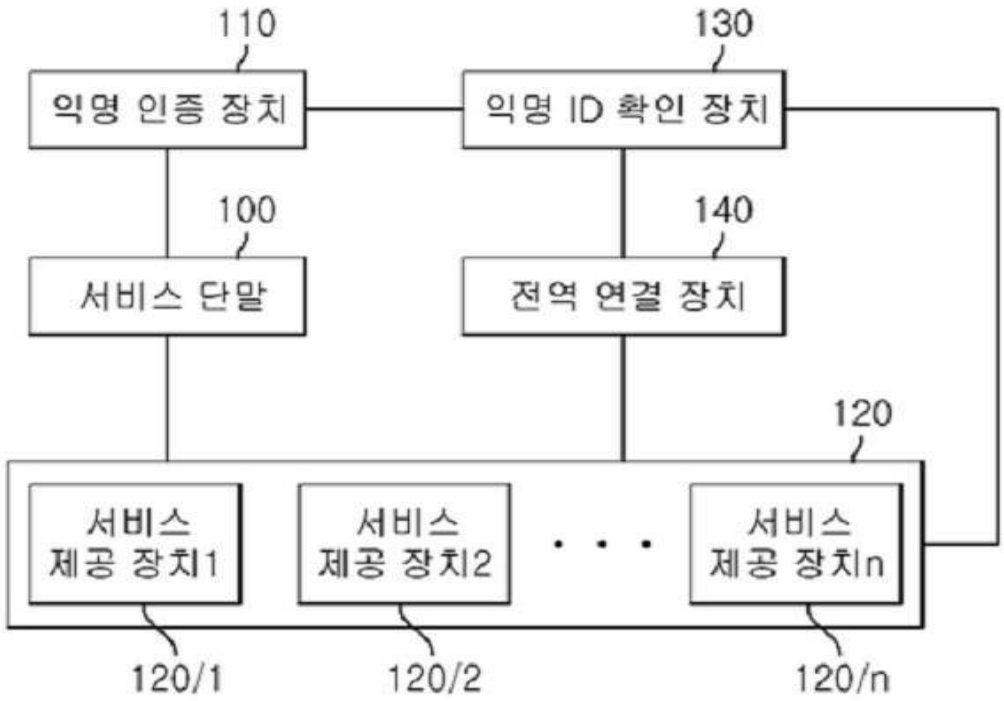
120: 익명 ID 확인 장치

130: 서비스 제공 장치

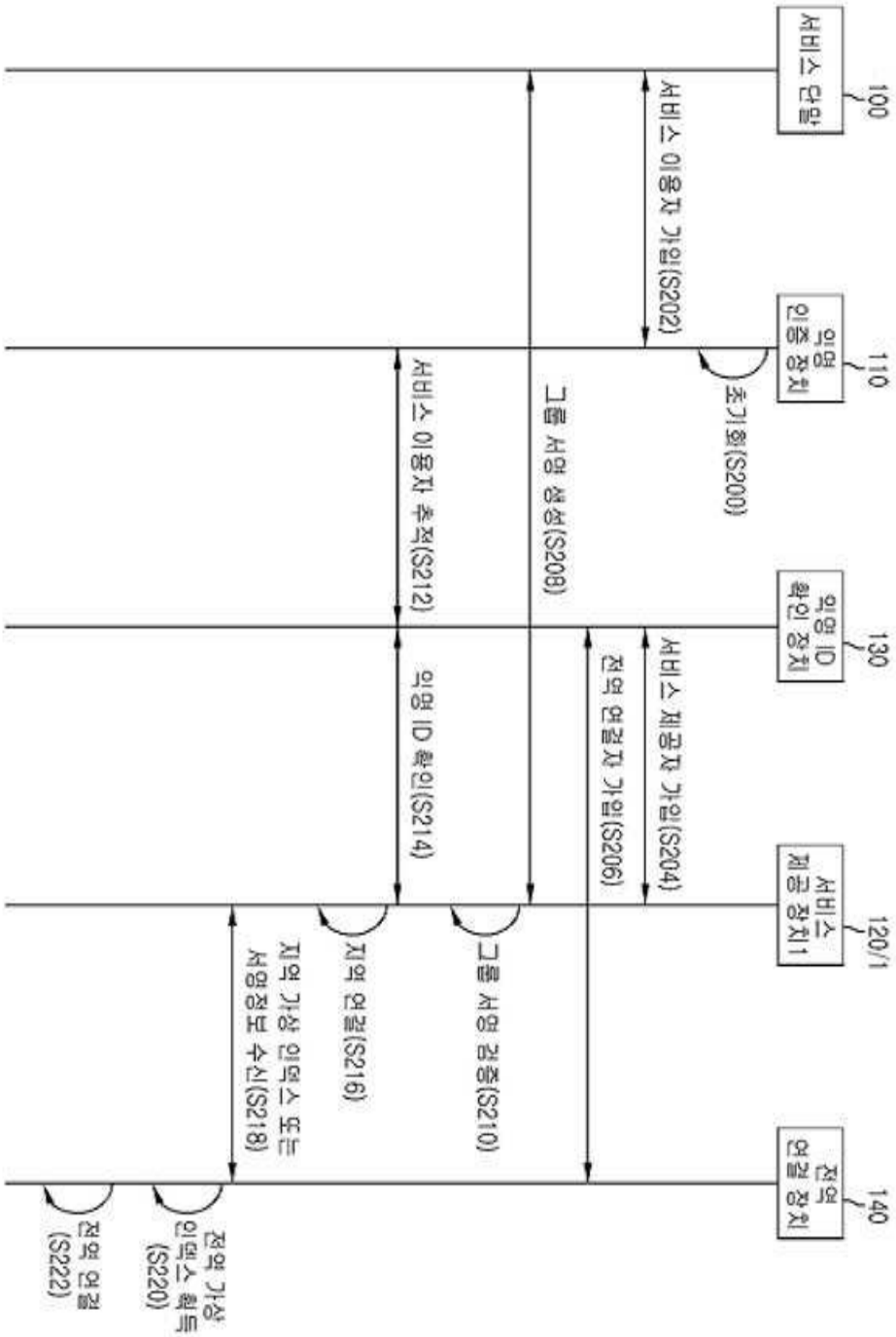
140: 전역 연결 장치

도면

도면1


110
익명 인증 장치
130
익명 ID 확인 장치
100
서비스 단말
140
전역 연결 장치
120
서비스 제공 장치1
서비스 제공 장치2
서비스 제공 장치n
120/1
120/2
120/n

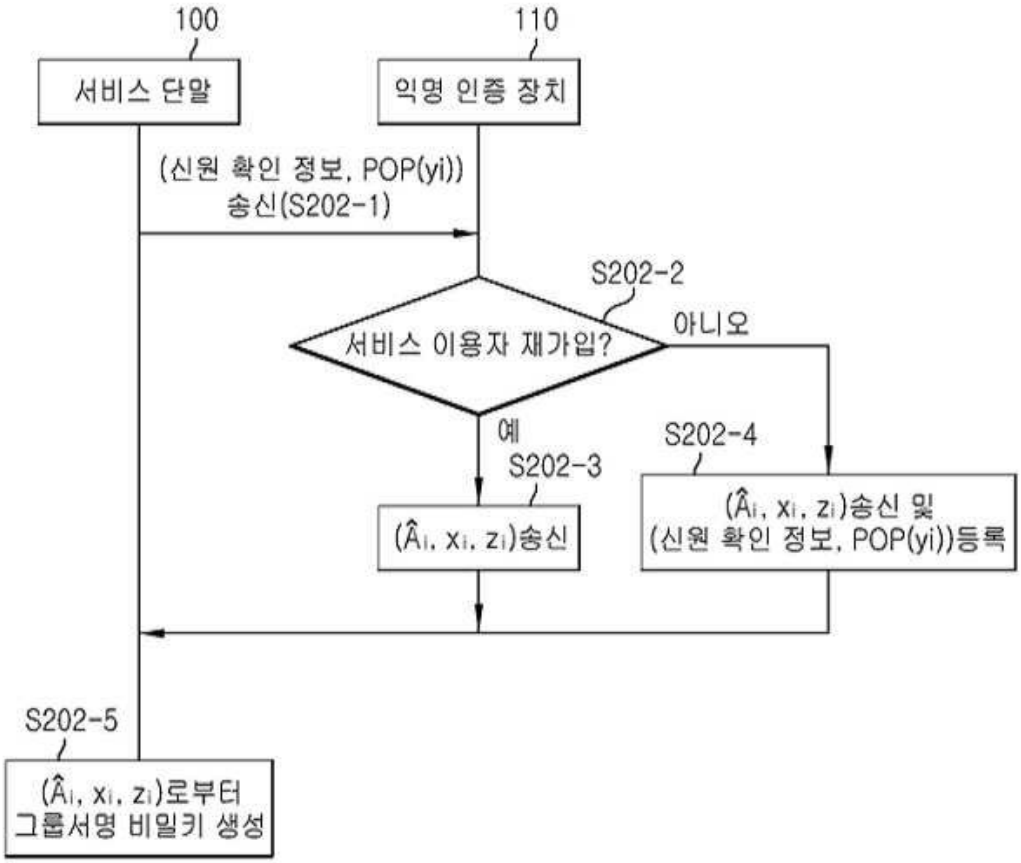
도면2


서비스 단말
100
서비스 이용자 가입(S202)
익명 인증 장치
110
초기화(S200)
그룹 서명 생성(S208)
서비스 이용자 추적(S212)
익명 ID 확인 장치
130
서비스 제공자 가입(S204)
전역 연결자 가입(S206)
익명 ID 확인(S214)
서비스 제공 장치1
120/1
그룹 서명 검증(S210)
지역 연결(S216)
지역 가상 인덱스 또는 서명정보 수신(S218)
전역 연결 장치
140
전역 가상 인덱스 획득 (S220)
전역 연결 (S222)

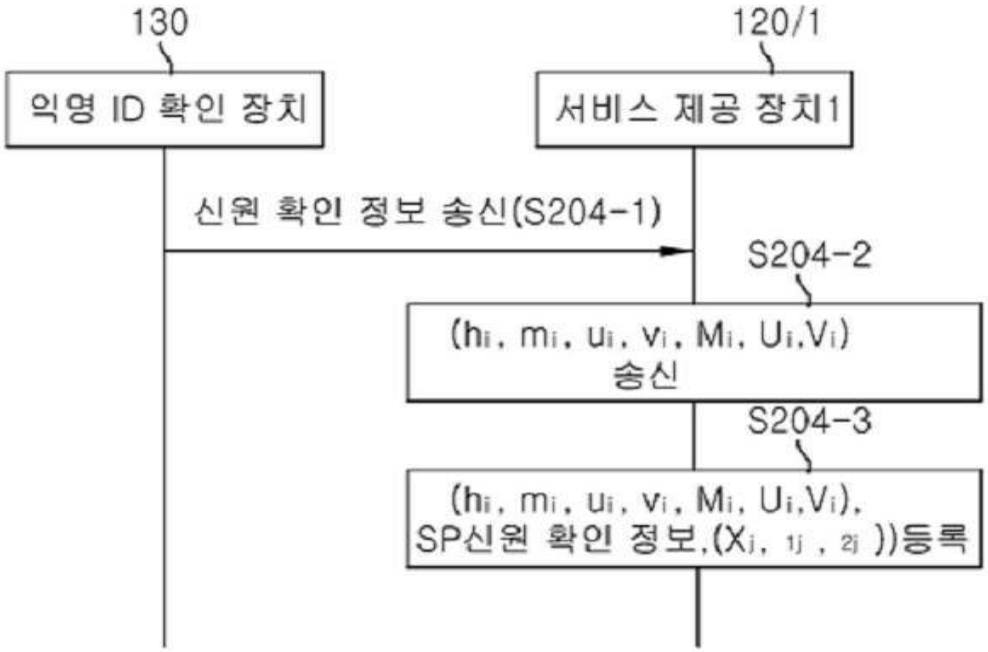
도면3


그룹공개 파라메터 생성
gpk=(e,G1, G2, g1, g2, g3, g4, w)
S200-1
그룹공개 파라메터 공개
S200-2

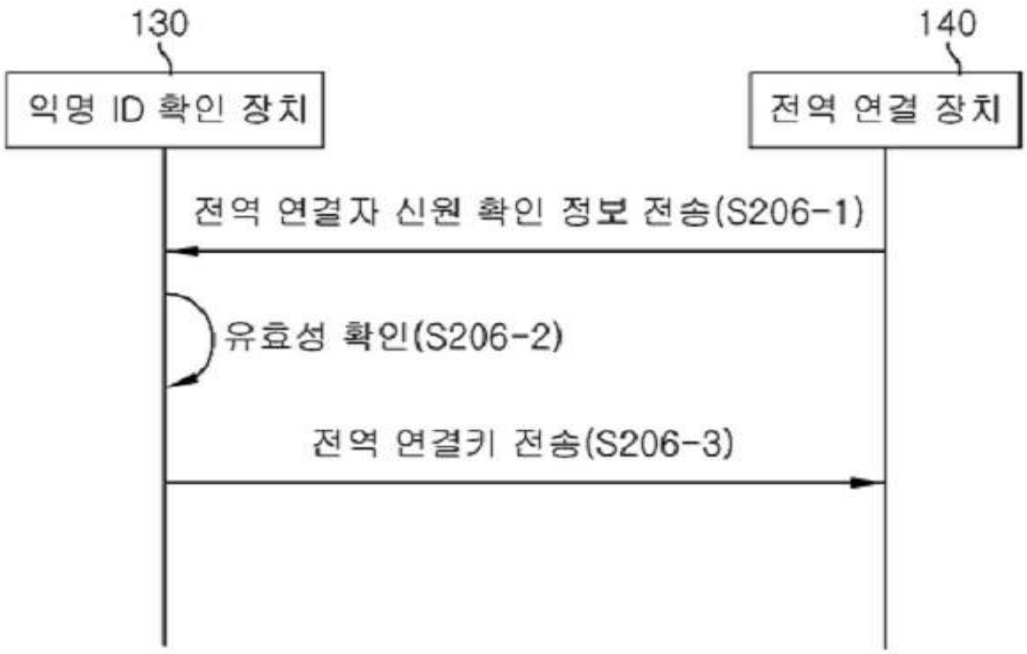
도면4


100
서비스 단말
110
익명 인증 장치
(신원 확인 정보, POP(yi))
송신(S202-1)
S202-2
서비스 이용자 재가입?
아니오
예
S202-3
(Âi, xi, zi)송신
S202-4
(Âi, xi, zi)송신 및
(신원 확인 정보, POP(yi))등록
S202-5
(Âi, xi, zi)로부터
그룹서명 비밀키 생성

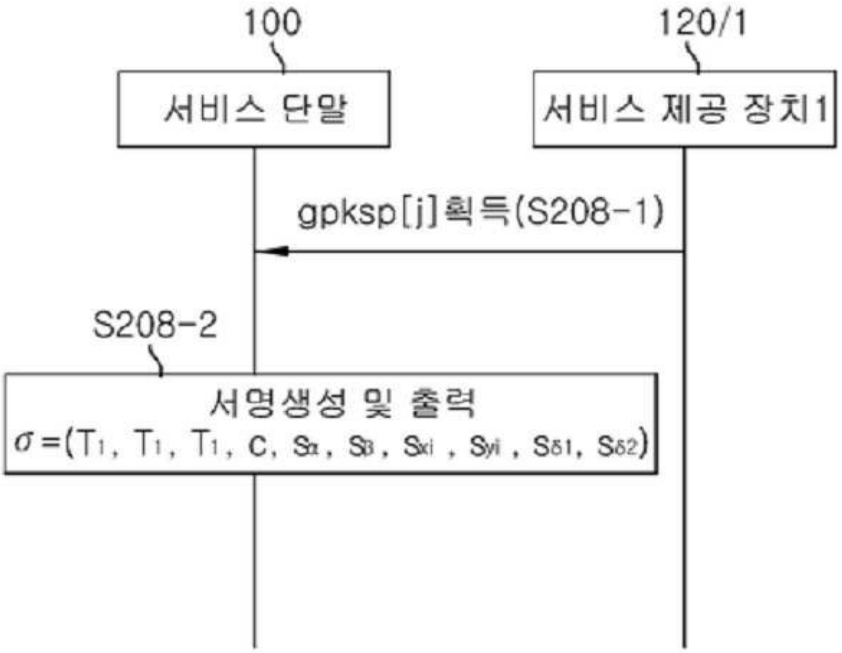
도면5


130
익명 ID 확인 장치
120/1
서비스 제공 장치1
신원 확인 정보 송신(S204-1)
S204-2
(hi, mi, ui, vi, Mi, Ui,Vi)
송신
S204-3
(hi, mi, ui, vi, Mi, Ui,Vi),
SP신원 확인 정보,(Xi, 1j , 2i))등록

도면6


130
익명 ID 확인 장치
140
전역 연결 장치
전역 연결자 신원 확인 정보 전송(S206-1)
유효성 확인(S206-2)
전역 연결키 전송(S206-3)

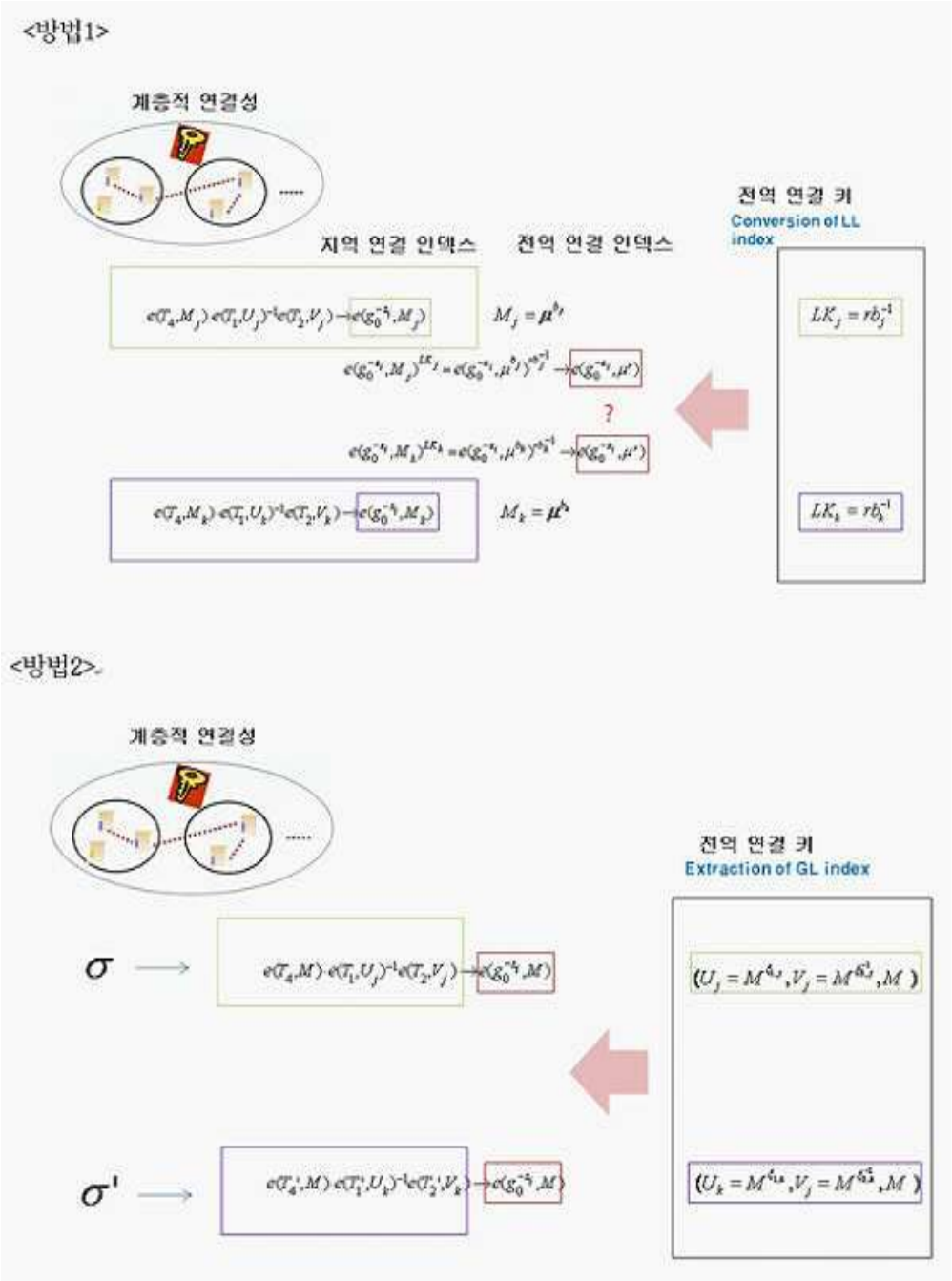
도면7


100
120/1
서비스 단말
서비스 제공 장치1
gpksp[j]획득(S208-1)
S208-2
서명생성 및 출력
σ=(T1, T1, T1, C, Sα, Sβ, Sxi, Syi, Sδ1, Sδ2)

도면8


서비스 이용자의 가상인덱스 계산
P=e(Ai, Mj)=e(g1^-Zi, MJ)
S216-1
가상 인덱스 등록
S216-2

도면9


<방법1>
계층적 연결성
지역 연결 인덱스
전역 연결 인덱스
전역 연결 키
Conversion of LL index
?
<방법2>
계층적 연결성
전역 연결 키
Extraction of GL index