通信情報保護學會論文誌
第 6 卷 第 1 號, 1996. 3

안전하고 효율적인 익명 통신로

박 춘 식*

Secure and Efficient Anonymous Channel

Choonsik Park*

요 약

본 논문에서는 Eurocrypt'93에서 제안된 효율적인 익명 통신로에 대한 Pfitzmann의 공격에 주안점을 두어, 그 공격에 대한 대책을 고려한 새로운 방식을 제안하고자 한다. 제안 방식은 송신자가 보내는 암호문의 크기가 다소 증가되는 점이 있으나, 이전의 방식과 동일하게 Mix 센터의 수에는 의존하지 않는다. 특히, 이전의 방식에서 필요로 했던 동시 동보 네트워크(simultaneous broadcast network)는, 제안된 방식에서는 고려하지 않고도 효율적으로 익명 통신로를 구현할 수 있다.

Abstract

In this paper, we focus on Pfitzmann's active attack against an efficient anonymous channel which was proposed at Eurocrypt'93 and show how the attack can be countered. In the new scheme to prevent the attack, the size of ciphertext sent by each participant increase somewhat, but, as in the previous scheme, its size does not depend on the number of mixes. In particular, the simultaneous broadcast network is now not required which was needed to open the results computed by each mix in the previous scheme.

1. 서 론

최근 군사 목적이나 외교용으로만 고려되어 오던 암호 기술이 급속한 정보화의 도래로 상업용으로도 크게 각광을 받고 있는 것은 주지의 사실이다. 특히 공개키 암호라는 새로운 개념의 암호 방식은 암호의 기능을 더욱 다양하게 만들었으며, 암호의 응용 분야를 크게 넓혀 왔다. 이들 중에서도, 암호를 이용한 전자 선거, 전자 현금, 전자 우편 등의 출현은 컴퓨터

* 한국전자통신연구소 부호기술연구부

네트워크를 통한 정보화 사회의 실현을 더욱 앞당기게 되었다. 그러나 대규모 컴퓨터 데이타 베이스에 보관, 저장되어 관리되는 개인의 정보에 대한 프라이버시 노출 위험, 이동 통신에서의 자신의 이동 위치 추적에 따른 개인의 사생활 침해, 통신 판매를 통한 개인의 취향 노출, 전자 현금 사용에 의한 개인의 재산 상태 등의 비밀 노출, 개인의 각종 정보를 IC 카드에 수록하여 증명서로 사용함에 따른 분실 및 특정 그룹에 의한 악용 등 너무나 많은 역기능 등이 우려되고 있다. 이러한 프라이버시를 보호하여 정보화 사회에 따른 역기능을 방지하는 데 이용될 수 있는 효율적이고 안전한 암호학적 수단으로, 익명 통신로(Anonymous Channel)가 있으며 이에 대한 많은 연구가 되어 왔다. 또한 이러한 익명 통신로는 트래픽 분석(Traffic Analysis)에 대한 보호 대책으로써도 별도로 연구되어 왔다[3][8].

익명 통신로는 그림 1에서 보는 바와 같이 참여자가 자신의 정보를 임의의 통신로에 보내었을 경우, 제3자에 의해서 자신과 자신이 보낸 메세지와의 대응 관계가 노출되지 않아 자신의 프라이버시를 지킬 수 있는 통신로를 말한다. 이러한 익명 통신로는 전자 선거, 전자 현금, 전자 우편 등의 프라이버시 기능을 제공해야하는 분야에 널리 활용되게 되었으며, D.Chaum이 제안한 Mix형 익명 통신로[3]가 가장 최초로 그 이후에도 많은 익명 통신로들이 제안되어 왔다[1][7][9][11][12].

그러나 이러한 익명 통신로에 대한 공격도 별도로 제안되어 왔다. 특히 Pfitzmann은 이러한 익명 통신로에 대한 공격으로, 먼저 Mix형 익명 통신로에 대한 공격[5]을 그리고 Shuffle형 익명 통신로에 대한 공격[6]을 차례로 제안한 바 있다. 본 논문에서는 Shuffle형 익명 통신로에 대한 Pfitzmann의 공격에 주안점을 두어, 그 공격에 대한 대책을 고려한 새로운 방식을 제안한다. 새로운 제안 방식은 송신자가 보내야 하는 암호문의 크기가 다소 증가하는 단점이 있으나, 이전의 방식과 동일하게, Mix 센터의 수에는 의존하지 않는다는 장점이 있다. 특히, 제안된 방식에서는 이전 방식에서 필요로 한 동시 동보 네트워크(Simultaneous broadcast network)를 고려하지 않고도 효율적으로 익명 통신로를 구현할 수 있음을 보인다.

본 논문은 모두 7개 장으로 구성된다. 2장에서는 본 논문에 사용된 용어의 정의와 공개키 암호 시스템의 기본적인 사항을 언급한다. 기존의 익명 통신로들을 3장에서 고찰해보고, 4장에서는 Shuffle형 익명 통신로에 대한 Pfitzmann의 공격을 소개한다. 5장에서는 Pfitzmann의 공격에 대한 대책과 개선된 방식

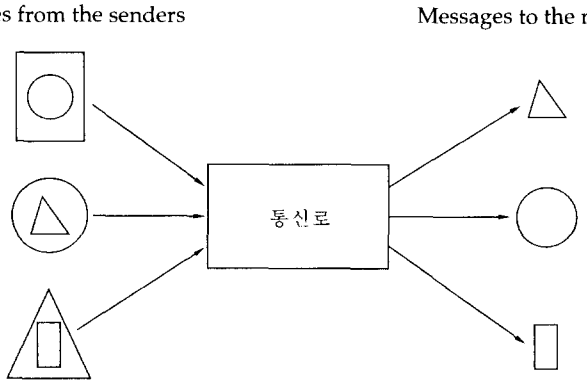

그림 1 익명 통신로

을 제안하고, 새로운 방식의 안전성에 대해서는 6장에서 다루기로 한다. 마지막으로 결론 부분을 7장에 다루었다.

2. 준 비

2.1 정의

먼저, 본 논문에서의 모든 통신은 공개 보드(public board)를 이용하여 행하는 것으로 가정한다.

■ **정의 1** 채널은 공개 보드와 확률적 다항식 시간 튜링 머신(*probabilistic polynomial time Turing machines*)($A_1, \cdots, A_n, S_1, \cdots, S_k$)로 구성된다. 단, A_i는 송신자이며 S_i는 *Mix* 센터이다. A_i와 S_i는 또한 참가자(*player*)라고도 한다.

■ **정의 2** 정의 1에 의한 채널이 다음과 같은 조건들을 만족할 때 익명 통신로라고 한다.

먼저, m_i는 A_i의 입력으로 그리고 $(o_1, \cdots, o_n)$을 공개 보드의 최종 리스트의 출력으로 한다.

Completeness : 만약 모든 참가자가 honest하다면,

$$\{o_1, \cdots, o_n\} = \{m_1, \cdots, m_n\}.$$

Privacy : 어떠한 i에 대해서도, A_i와 m_i의 대응 관계는 비밀로 지켜져야 한다.

본 논문에 사용되는 ∘는 연접(concatenation)을, ⊕는 bitwise exclusive OR을 그리고 $|x|$는 x의 길이를 의미한다.

2.2 공개키의 기본적인 사용

E_A를 Alice의 공개키로, E_A^{-1}를 비밀키로 할 경우 임의의 X에 대해서, 다음 식이 만족한다고 가정한다.

$$E_A{}^{-1}E_A(X) = E_AE_A{}^{-1}(X) = X. \quad (1)$$

메세지 M은 다음과 같이 암호화 된다.

$$C = E_A(M \circ R) \quad (2)$$

단, R은 난수이다. 여기서 R이 사용되는 이유는 다음과 같다. 난수 R를 사용하지 않은 식 (3)과, $\{C_i\}(i = 1, \cdots, n)$와 $\{M_i\}(i = 1, \cdots, n)$가 공격자(adversary)에게 주어졌다고 가정해 보자.

$$C_i = E_A(M_i) \ (1 \le i \le n) \quad (3)$$

이때, 공격자(adversary)는 식 (3)을 이용하여 $\{C_i\}$과 $\{M_i\}$의 대응 관계를 쉽게 찾을 수 있다. 이러한 대응 관계를 숨기기 위해서, 난수 R이 식 (2)에서 필요하게 된다.

3. 기존의 익명 통신로

본 절에서는 기존의 익명 통신로인, Mix형 익명 통신로[3], DC(Dining Cryptographers)형 익명 통신로[4] 그리고 Shuffle형 익명 통신로[7]에 대해서 설명한다.

3.1 Mix형 익명 통신로

k개의 Mix 센터를 사용하는 Chaum의 Mix형 익명 통신로[3]는 다음과 같다. n명의 송신자를 $A_1, \cdots, A_n$라 하고, 각각의 송신자 A_i는 A_i와 m_i의 대응 관계를 비밀로 유지한 채, 메세지 m_i를 안전하게 전송하고자 한다. 수신자 B_i의 공개키를 E_{B_i}라 하고 센터 S_i의 공개키를 E_i이라고 한다. 여기서, 센터 S_i의 역할은 각 송신자의 암호문을 복호화하여, 난수 성분을 제거한 후 그 결과를 알파벳순으로 순서를 바꾸어 출력하는 것이다.

[Chaum의 Mix형 익명 통신로]

[step 1] 각 송신자 A_i는 k개의 난수 $R_1, \cdots, R_k$를 발생하여, 다음과 같은 암호문을 계산한 후 공개 보드(Public board)에 전송한다.

$$E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{B_i}(m_i)) \cdots))$$

(step 1은 A_i가 메세지, $B_i \circ E_{B_i}(m_i)$를 Mix 익명 통신로에 보낸다고 하는 의미이다.)

[step 2] 최초의 Mix S_1는 수신한 암호문들을 복호화하고, 그 내용중에서 난수 R_1을 제거한 후, 남은 내용들을 알파벳 순으로 나열하여 공개 보드에 전송한다.

$$E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{B_i}(m_i)) \cdots)$$

[step 3] 마지막 Mix S_k를 제외한 나머지 Mix들 $S_2, \cdots, S_{k-1}$는 차례로 step 2와 같은 동작을 반복 수행한다.

[step 4] 마지막으로, S_k는 $\{B_i \circ E_{B_i}(m_i)\}$를 알파벳 순으로 나열하여 공개 보드에 전송한다.

Mix형 익명 통신로에서는 적어도 단 하나의 Mix만이라도 정직하다면, $\{A_i\}$와 $\{m_i\}$의 대응 관계는 나머지 다른 Mix들에게 조차도 비밀로 할 수가 있다. 즉, multi-party sender anonymity의 기능을 실현하게 된다.

3.2 DC(Dining Cryptographers)형 익명 통신로

D.Chaum은 Mix형 익명 통신로와는 그 성격이 서로 다른 DC(Dining Cryptographers)형 익명 통신로[4]를 제안하였다. DC형 익명 통신로는 무조건 안전(unconditional secure)한 sender anonimity로, 참가자중의 한 사람이 익명으로 메세지를 보낼 수 있도록 모든 참가자가 동시에 자신의 암호문을 전송하는 방식이다.

먼저 n명의 송신자를 $A_1, \cdots, A_n$이라 하고 각 송신자 A_i는 A_i와 자신의 메세지 m_i와의 대응 관계가 비밀로 유지된 채, 메세지 m_i를 전송하고 싶다고 하자. 준비 단계로 각 A_i는 n개의 난수 K_{ij}, $i \neq j$, $j = 1, \cdots, n$를 발생하여, 다른 송신자들에게 비밀 통신로를 통하여 사전 분배한다. 여기서, K_{ij}는 두명의 i와 j만이 알게 되는 비밀키가 된다. DC형 익명 통신로는 다음 프로토콜에 의해서 실현될 수 있다.

[DC형 익명 통신로]

[step 1] 각 송신자 A_i는 자신이 발생한 K_{ij}, 다른 송신자들로 부터 수신한 모든 키 K_{ji} 그리고 자신이 보내고 싶은 메시지 m_i를 모두 합한 값을 계산한다. 이때 보낼 메세지가 없는 송신자는 m_i 대신에 $m_i = 0$로 한 합을 계산한다.

[step 2] 각 A_i는 step 1에서 계산한 다음의 값, V_i를 공개 보드에 전송한다.

$$V_i = m_i \oplus K_{ij} \oplus K_{ji}$$

[step 3] 모든 송신자가 보낸 메세지 V_i의 합은 누구에 의해서도 쉽게 계산될 수 있다. 모든 키가 두번씩 더하여 지기 때문에, 단 한사람만이 메세지를 보낸 경우 이 계산 결과는 그 사람이 보낸 메세지가 되게 된다.

DC형 익명 통신로에 있어서, 모든 송신자들이 보낸 출력의 합이 주어지거나 또는 각 송

신자의 출력이 주어졌을 때, 메세지를 발신한 송신자를 찾는 것은 어려운 일이다.

3.3 Shuffle형 익명 통신로

RSA 공개 키 암호[2]를 사용한 Chaum의 Mix형 익명 통신로는 각 송신자가 보내어야만 하는 암호문의 길이가 아주 길다. 암호문, $E_1(R_1 \circ E_2(R_2 \cdots E_k(R_k \circ B_i \circ E_{R_i}(m_i)) \cdots))$의 길이는 센터의 수, 즉 Mix의 수 k에 따라 늘어나게 된다. 이러한 문제를 극복하기 위하여, RSA 암호 대신에 ElGamal 공개키 암호[1]를 이용한 효율적인 익명 통신로를 Park 등이 제안하였다[7]. Park 등이 제안한 Shuffle형 익명 통신로는 추적 불능 시스템용의 Type-1형 익명 통신로와 전자 선거용의 Type-2형 익명 통신로로 나누어져 있다.

3.3.1 Type-1형 익명 통신로

Shuffle형 익명 통신로는 ElGamal 암호 방식을 이용한다. 권한있는 당국이나 신뢰할 만한 센터는 (q, g)를 생성, 공개한다. 여기서 q는 소수이며, g는 $GF(q)$ 상의 원시근(primitive element)이다. 각 센터 S_i가 사용하는 관련 키는 다음과 같다.

(**Secret key of** S_i) $X_i \in \{1, \cdots, q-1\}$

(**Public key of** S_i) $Y_i (= g^{X_i} \bmod q)$

(S_i는 X_i를 택한 후 Y_i를 공개한다.)

Type-1형 익명 통신로는 Mix형 익명 통신로의 용어들을 그대로 사용하며, 그 프로토콜은 다음과 같다.

[Type-1 Anonymous Channel]

[step 1] 각 송신자 A_i는 난수 R을 선택하여 아래의 (C_{0i}, C_{1i})를 계산한다.

$$(C_{0i}, C_{1i}) \triangleq (g^R, m_i \times (Y_1 \cdots Y_k)^R)$$

A_i는 이들 (C_{0i}, C_{1i})를 공개 보드에 보낸다. 여기서 $f_j(t, u, r)$를 다음과 같이 정의한다.

$$f_j(t, u, r) \triangleq \begin{cases} (t \times g^r,\ u \times (Y_{j+1} \cdots Y_k)^r \Lambda^{X_j}) & \text{if } 1 \le j \le k\text{-}1 \\ u \Lambda^{X_k} & \text{if } j = k \end{cases}$$

$i = 1, \cdots, k$에 대해서 다음을 수행한다.

[step 2]

$(t_1, u_1), (t_2, u_2), \cdots, (t_n, u_n)$

을 공개 보드에 마지막으로 남는 각 송신자 A_i의 출력 list라고 하자. S_i는 난수들 $r_1, \cdots, r_n$를 생성하여 $j = 1, \cdots, n$에 대해서 $f_j(t_j, u_j, r_j)$를 계산한다.

[step3] S_i는 $\{f_j(t_j, u_j, r_j)\}$ $(j = 1, \cdots, n)$를 공개 보드에 알파벳 순으로 순서를 바꾸어 출력한다.

마지막으로 공개 보드에는 알파벳 순서로 나열된 출력 list, $\{m_i\}_{i=1, \cdots, n}$가 남게 된다.

상기의 프로토콜에서, (C_{0i}, C_{1i})는 난수 R_1, $\cdots$, R_{k-1}에 대해서 다음과 같이 변경되어 간다.

$$\begin{aligned} (C_{0i}, C_{1i}) &= (g^R, m_i \times (Y_1 \cdots Y_k)^R) \\ &\rightarrow (g^{R_1}, m_i \times (Y_2 \cdots Y_k)^{R_1}) \\ &\quad \vdots \\ &\rightarrow (g^{R_{k-1}}, m_i \times (Y_k)^{R_{k-1}}) \\ &\rightarrow m_i \end{aligned}$$

3.3.2 Type-2형 익명 통신로

Type-1형 익명 통신로를 전자 선거에 사용하기 적합한 형태로 바꾼 Type-2형 익명 통신로는 다음과 같다. 먼저, Type-2형 익명 통신로에 필요한 관련 함수들을 먼저 정의한다. m를 평문으로 할 경우 모든 Mix 센터의 공개키를 이용하여 계산한 암호문은 다음과 같다.

$$E(m,r) \triangleq (g^r,\ m\times(Y_1\cdots Y_k)^r) \bmod q.$$

단, r는 난수이다.

센터의 키 관련 정보나 공개 정보는 Type-1형과 같으며, 모든 S_i는 암호문들을 복호화 하기 위해서는 동시 동보 네트워크(simultaneous broadcast network)를 이용하는 복호화 프로토콜이 필요하다. a와 b를 다음과 같이 정의할 때, 복호화 프로토콜은 다음과 같다.

$$a \triangleq g^r \bmod q,$$
$$b \triangleq m\times(Y_1\cdots Y_k)^r \bmod q.$$

[Decryption Protocol]

[step 1] S_i는 $Z_i = a^{X_i}(= (g^r)^{X_i} = Y_i^r \bmod q)$를 계산하고 이를 공개한다. 이때, 각 S_i는 다른 Mix 센터, S_j가 공개한 Z_j를 본 후, 자신의 Z_i를 공개하는 것을 방지하기 위해서 동시 동보 네트워크를 통하여 Z_i가 동시에 공개되도록 한다.

[step 2] 누구든지 쉽게 평문 m을 복원할 수 있다.

$$b/(Z_i\cdots Z_k) = m\times(Y_1\cdots Y_k)^r/(Z_1\cdots Z_k) = m.$$

$f(a,b,e)$를 다음과 같이 정의하면 아래의 보조 정리를 쉽게 얻을 수 있다.

$$f(a,b,e) \triangleq (a\times g^e,\ b\times(Y_1\cdots Y_k)^e) \bmod q.$$

보조정리 1 만일 $(a,b) = E(m,r)$이면, $f(a,b,e) = E(m,r+e)$이다.

[Type-2 Anonymous Channel]

[step 1] 각 송신자 A_i는 $E(m_i, r_i)$를 계산하여 공개 보드에 보낸다. 단, r_i는 난수이다.

[step 2] S_1는 난수 $e_1, e_2, \cdots, e_n$를 발생하여, 각 i에 대하여 다음을 계산한다.

$$f(E(m_i, r_i), e_i) = E(m_i, r_i + e_i)$$

S_1는 $\{E(m_i, r_i + e_i)\}$를 알파벳 순으로 나열하여 공개 보드에 보낸다.

[step 3] $S_2 \sim S_k$는 차례로 Step 2를 수행한다. 수행이 완료되었을 때, 알파벳 순으로 나열된 출력 list $\{E(m_i, x_i)\}$를 얻게된다. 여기서, x_i는 난수이다.

[step 4] $S_1 \sim S_k$는 복호화 프로토콜(Decryption Protocol)을 수행하여 $\{m_i\}$를 얻을 수 있다.

여기서 $|(C_{0i}, C_{1i})| = 2 \times |q|$로 일정하므로 센터의 수에 따라 암호문 길이가 증가하게 되는 Mix형 익명 통신로의 문제점은 Type-1형과 Type-2형 익명 통신로에서는 존재하지 않게 된다.

3.4 익명 통신로의 비교 분석

이상에서 각 익명 통신로에 대한 내용들을 분석하여 보았다. 이 절에서는 각각의 익명 통신로에 대하여, 사용한 암호, 구성 방법, 문제

점 등에 대해서 간략히 표 1로 정리하였다. 표 1의 DC형 익명 통신로에 대한 공격 방법은 아직까지 알려져 있지 않다.

4. Shuffle형 익명 통신로에 대한 Pfitzmann의 공격

Eurocrypt'94 암호 학회에서 Pfitzmann은 Shuffle형 익명 통신로가 안전하지 못함을 지적한 바 있다[6]. Pfitzmann의 공격은 Type-1형과 Type-2형 익명 통신로 모두에 적용될 수 있는 공격으로 수동적인 공격(Passive Attack)과 능동적인 공격(Active Attack)으로 되어 있다. 수동적인 공격은 Pfitzmann[6]의 논문에서 지적한 대로 간단히 방지할 수 있으므로, 본 논문에서는 Type-1형 익명 통신로에 대한 능동적인 공격만을 고려한다. Pfitzmann의 능동적 공격은 먼저 공격의 전제 조건으로, 두 Mix 센터(맨 처음 센터와 맨 마지막 센터)는 송신자중의 한 송신자와 사전에 결탁하여야 한다.

이 공격의 목적은 맨 마지막 Mix 센터의 출력과 맨 처음 Mix 센터의 입력 사이의 관계를 찾는 즉, 송신자와 송신자가 보낸 메세지와의 대응 관계를 알려고 하는 것이다. 이렇게 될 경우, 결국 Shuffle형 익명 통신로는 안전하지 못하게 된다.

Type-1에 대한 Pfitzmann의 공격은 다음과 같다. 한명의 송신자 A_h, 그리고 두 Mix 센터 S_1과 S_k를 공격자라 하고, 그들은 어떤 송신자 A_j의 비밀 메세지를 알기 위하여 사전에 결탁한다고 가정한다. 여기서 A_j가 보낸 암호문을 $C_j = (g^R, m_j \times (Y_1 \cdots Y_k)^R)$이라고 하자. 단, R는 난수이고 Y_i는 각 Mix 센터의 공개키이다.

[step 1] 공격자 S_1(맨 처음 Mix 센터)는 A_j가 보낸 암호문 C_j를 이용하여 먼저 $C'_j = (C'_{0j}, C'_{1j}) = (g^{R+r}, m_j \times (Y_2 \cdots Y_k)^{R+r})$를 계산한다. 다음으로, 공격자들 사이에서 사전에 약속된 u를 이용하여 다음과 같은 암호문을 발생한다.

$$C''_j = (C''_{0j}, C''_{1j}) = (g^{R+r}, m_j^u \times (Y_2 \cdots Y_k)^{R+r})$$

송신자들로 부터 수신한 나머지 암호문들에 대해서는, S_1는 정상적인 동작을 수행한다.

표 1 익명 통신로의 비교

	Mix[3]	DC[4]	Shuffle[7]
1. 사용 암호	RSA	비밀 키 방식	ElGamal
2. 구성 방법	복수개 센터 Cascade Type	방송형 Net. Broadcast Type	복수개 센터 Cascade Type
3. 전송 용량	센터수에 의존	대량	일정
4. 안전성	Computational Secure	Unconditional Secure	Computational Secure
5. 공격 방법	Pfitzmann[5]	알려져 있지 않음	Pfitzmann[6]
6. 문제점	전송 메세지의 증가 insecure	비밀키 사전 분배 메세지 충돌[10]	Type-1은 insecure Type-2는 secure
7. 용도	전자 선거, 전자 메일 등	전자 선거 등	전자 선거, 전자 메일 등

[step 2] S_1는 A_b의 중간 결과인 C'_b 대신에 step 1에서 계산한 C''_j로 대치하여 변형되지 않은 다른 중간 결과들과 함께 공개 보드에 출력한다.

[step 3] S_k를 제외한 나머지 Mix 센터들, S_2, …, S_{k-1}는 Type-1형 익명 통신로에서와 같이 동일한 일을 차례로 수행한다.

[step 4] 마지막 Mix 센터 S_k는 먼저 $i = 1$, …, n에 대해서 m_i를 계산해내고 그 계산된 결과에 u승을 한, m_i''를 다른 결과 m_j와 비교한다. 만일, 그 결과들이 일치할 경우에는 S_k는 A_i의 비밀 메세지 m_j를 찾을 수가 있다. 결국 m_i와 m_j''를 얻게 되어 m_j와 A_i가 보낸 암호문, C_i의 대응 관계를 알게된다.

[step 5] 마지막으로, S_k는 m_j''를 m_b(사전에 A_b와 약속된 메세지)로 바꾼 후 최종 출력들을 공개 보드에 출력한다. 결국 어느 누구도 공격이 행하여 졌는 지를 알 수 없게 된다.

참고 1 공격자 Mix 센터 S_1는 C'_j가 A_j의 비밀 메시지를 포함하고 있다는 것을 알고 알파벳 순으로 출력을 내어 보낼 때, 이미 결탁한 송신자 A_b에 해당하는 중간 결과 C'_b를 빼어버리고 대신에 step 1에서 계산한 C''_j를 출력으로 내어 보내어야 한다. 만일, 이와 같이 하지 않을 경우는 공개 보드의 크기가 변화됨으로 인해 다른 참가 송신자들에 의해 Pfitzmann의 공격은 쉽게 발각되기 때문이다.

참고 2 Type-2에 대한 Pfitzmann의 공격은 Type-1의 공격과 아주 유사하다. 그러나, 동시 동보 네트워크(Simultaneous Broadcast Network)가 Type-2형 익명 통신로에는 사용되기 때문에 Type-2형 익명 통신로는 Pfitzmann의 이러한 공격에 대해서는 아직도 안전하다.

5. Pfitzmann의 공격에 안전한 새로운 방식

Shuffle형 익명 통신로에서 만일 마지막 Mix 센터가 정직하고(부정한 행위를 하지 않고 결탁하지 않는) 그리고 보내고자 하는 메세지에 각 송신자들이 일정한 형태의 포맷을 첨부한다면, Pfitzmann의 공격은 쉽게 방지될 수 있다. 그러나 이러한 가정은 마지막 Mix 센터가 신뢰될 수 있다면 나머지 Mix 센터를 사용할 필요가 없기 때문에 공격에 대한 안전 대책으로는 도움이 되지 못한다. 그래서 이러한 방법이 아닌 형태로 Pfitzmann의 공격을 피할 수 있는 보다 안전하고 실용적인 방식을 제안한다.

5.1 기본적인 대책

Shuffle형 익명 통신로의 취약점은 맨 처음 Mix 센터가 임의로 출력을 변경하거나 그리고 마지막 Mix 센터가 변형된 메세지와 원래의 메세지 사이의 대응 관계를 찾을 수 있다는 것이다. 이러한 대응 관계를 찾을 수 없도록 하는 하나의 대책으로 먼저 보내고자 하는 메세지에 잉여 정보(redundancy information)를 첨부하고 그것을 암호화한 값을 송신자의 메세지로서 보내도록 하는 것이다. 즉, Shuffle형 익명 통신로에서의 메세지 m, 대신에 다음과 같은 메시지 M를 보내는 것이다.

$$M = E(\overbrace{m \circ \textit{redundant data}}^{l}) \circ \overbrace{\textit{redundant data}}^{l}$$

단, E는 암호화 과정이며, redundant data는 l 비트의 one way hash 함수의 결과를 사용하면 된다.(l 비트의 크기는 안전성과 관련된 변수이다.)

Shuffle형 익명 통신로 (Type-2)에 잉여 정보를 사용하는 대책을 수립하면 Pfitzmann의 공격은 쉽게 발견될 수 있다. 그러나 만일 공격자가 자신의 신분이 노출됨에도 불구하고 공격을 강행한다면 메세지와의 대응 관계를 찾을 수 있는 가능성이 있다. 그러나, 원래의 메세지 대신에 위에서 설명한 바와 같이 암호문과 잉여 정보를 보냄으로써 잉여 정보의 내용이 틀릴 경우, 공격자들이 알게되는 내용은 오로지 암호문뿐이므로 이러한 공격에도 제안 방식에서는 쉽게 대처할 수 있다. 즉 암호문에 추가된 잉여 정보의 오류가 발견되지 않을 경우만 원래의 메시지가 복원될 수 있으며, 오류가 발견될 경우는 암호문 밖에 알 수 가 없게 된다.

또 다른 대책으로 안전한 bit commitment 방식을 Type-2형 익명 통신로의 복호화 프로토콜(제안 방식에서는 Opening 단계)에 사용하는 것이다. 이로써 Type-2형 익명 통신로에서 사용했던 동시 동보 네트워크는 제안 방식에서는 필요하지 않게 된다. 이 대책으로 인하여 실제로 실현하기 곤란했던 동시 동보 네트워크의 구현 문제는 고려하지 않아도 가능하므로 제안 방식이 더욱 실용성을 가질 수 있게 되었다.

5.2 제안 방식

본 방식은 Shuffle형 익명 통신로에서 사용한 ElGamal 암호 방식을 그대로 사용하며 사용 파라메터는 다음과 같다.

(**Common information**) g, h, q_1, q_2

- q_1와 q_2는 $|q_1| > |q_2| + |l|$인 소수
- g와 h는 $GF(q_1)$과 $GF(q_2)$상의 원시근

(**Public keys of** S_i) $Y_i(= g^{X_i} \bmod q_1)$ 와 $W_i(= h^{V_i} \bmod q_2)$

(**Secret keys of** S_i) X_i와 V_i

(**Message of** A_i) m_i

(**Action of** A_i) 각 A_i는 난수 R를 발생하여 다음과 같은 형태의 암호문 C_i를 계산한다.

$$C_i = (C_{i0}, C_{i1}) \triangleq (g^R, \boldsymbol{M}_i \times (Y_1 \cdots Y_k)^R),$$

단, $\boldsymbol{M}_i$는 m_i의 암호문과 잉여 정보이다.

A_i는 공개 보드에 C_i를 보내게 된다.

제안 방식은 Type-2형 익명 통신로와 아주 유사하나 여기서는 두 단계로 즉 Shuffling 단계와 Opening 단계로 나누어 설명한다. Shuffling 단계의 최종 출력은 암호문 C_1, ⋯, C_n의 혼합된 형태이며, Opening 단계는 중간 결과들인 $\boldsymbol{M}_1$, ⋯, $\boldsymbol{M}_n$을 계산하여 그것에 첨부된 잉여 정보들의 정당성을 점검한다. 이 단계에서 오류가 발견되지 않을 경우, 원래의 메세지 m_1, ⋯, m_n이 계산되고 메세지에 첨부된 잉여 정보 또한 마지막으로 점검되게 된다.

[Shuffling stage]

먼저 각 송신자는 다음과 같은 암호문을 자신이 보내고자 하는 메세지 m_i를 이용하여 암호화한다.

$$\boldsymbol{M}_n = (h^t, (W_1 \cdots W_k)^t (m_i \circ H(m_i))) \circ H(Z)$$

단, H는 one way hash 함수, t는 난수이며, $Z = (h^t, (W_1 \cdots W_k)^t (m_i \circ H(m_i)))$이다. 각 송신자 A_i의 역할이 m_i 대신에 $\boldsymbol{M}_i$를 계산하는 것을 제외하고는 Type-2형 익명 통신로의 step 3

까지는 동일한 동작을 수행한다. 여기서 $(C_{0i}, C_{1i}) = (g^R, M_i \times (Y_1 \cdots Y_k)^R) (\mathrm{mod}\ q_1)$이며, $|(C_{0i}, C_{1i})| = 2 \times |q_1|$이다.

$$(\hat{\alpha}_1, \hat{\beta}_1), \cdots, (\hat{\alpha}_n, \hat{\beta}_n)$$

을 공개 보드에 남게 된 출력 list라고 하자. 이때 치환 $\pi : \{1, \cdots, n\} \rightarrow \{1, \cdots, n\}$와 난수 $d_1, \cdots, d_n$를 이용하여 다음과 같이 표현할 수 있다.

$$\hat{\alpha}_i = g^{d_i}$$
$$\hat{\beta}_i = M_{\pi(i)} \times (Y_1 \cdots Y_k)^{d_i}$$

[Opening stage]

$C(u, r)$는 u의 commitment를 나타내며 r는 난수를 나타낸다.

[step 1] 각 Mix 센터 S_i는 $Z_j^i \triangleq \hat{\alpha}_j^{X_i} (= Y_i^{d_i})$를 계산하고, $j = 1, \cdots, n$에 대한, $C_j^i = C(Z_j^i, r_j^i)$를 랜덤한 순서로 공개 보드에 출력한다.

[step 2] 모든 k개의 Mix 센터들이 commitments들을 다 보낸 후, 각 S_i는 모든 j에 대해서 C_j^i의 내용들을 공개한다.

[step 3] Z_j^i의 정당성은 누구에 의해서도 쉽게 확인되어지며, $M_j \triangleq \hat{\beta}_j / Z_j^1 \cdots Z_j^k$ 또한 쉽게 계산되어 진다. 이때, M_j의 잉여 정보, $H(Z)$의 정당성이 확인되어 진다.

[step 4] 만일 잉여 정보 테스트(redundancy test)가 모든 j에 대해서 성공적으로 통과한다면, 각 Mix 센터 S_i는 $\hat{Z}_j^i \triangleq (h^{t_i})^{V_i} (= W_i^{t_i})$를 계산하여 step 1과 step 2와 같은 방법으로 공개 보드에 출력한다.

[step 5] step 3과 같이 $m_j \triangleq \hat{\gamma}_j / \hat{Z}_j^1 \cdots \hat{Z}_j^k$는 계산되고, 잉여 정보, $H(m_j)$ 또한 점검된다. 여기서, $\hat{\gamma}_i \triangleq (W_1 \cdots W_k)^{t_i} (m_j \circ H(m_j))$이다.

만일 step 4에서 테스트가 실패하면 step 5를 더이상 수행하지 않거나, 영지식 상호 증명 시스템(Zero Knowledge Interactive System)을 이용하여 부정 행위를 한 Mix 센터나 송신자를 찾아내어 제거한 후 step 5를 수행하여 모든 프로토콜을 완료할 수도 있다.

6. 안전성 검토

제안 방식의 안전성에 대한 검토로서 가능한 공격들을 예상하여 그 공격에 안전함을 보이거나 약간의 추가 대책을 고려하면 안전하게 될 수 있음을 보인다.

먼저 Mix형 또는 Shuffle형 익명 통신로에 적용한 Pfitzmann의 공격[5],[6] 중에서 재 암호화 공격(Reencryption attack)과 직접 선택 공격(Direct chosen attack)을 고려한다. 재 암호화 공격은 모든 최종 출력들을 각 Mix 센터의 공개키로 암호화하고 이들을 송신자들로 부터의 최초 입력들과 비교하여 입출력간의 대응 관계를 찾는 공격이다. 이 공격에 대한 제안 방식의 대책은 각 Mix 센터가 수신한 암호문들을 복호화한 후, 새로운 난수를 그 암호문에 추가하고 그리고 이 결과를 랜덤한 순서로 다음 Mix 센터에게 전송하는 것이다. 즉, 2.2절에서 설명한 바와 같이, 각 Mix 센터에 의해 연접된 난수때문에 대응 관계를 찾기는 쉽지 않게 된다.

Mix형 익명 통신로에 적용된바 있는 직접 선택 공격[5]을 새로운 제안 방식에도 적용해 볼 수 있다. 이 공격은 부정한 송신자가 다른 송신자가 보내는 암호문을 본 후에, 그 암호문을 이용하여 공격을 시도하는 것으로, 이는 송

신자들이 그들의 암호문을 저장하여 지정된 시각에 일제히 보냄으로써 공격을 저지할 수 있다. 만일 송신자들이 암호문을 저장하여 동시에 보내는 것이 곤란할 경우는 전송전에 암호문에 Timestamp 정보를 부가하는 방법을 사용할 수 있다. 각 송신자가 $(Y_1 \cdots Y_k)^R \times M_i$를 보내는 대신에 timestamp 정보 T가 부착된 $C_{1i} = (Y_1 \cdots Y_k)^{R \times T} \times M_i$를 보내고, 맨 처음 Mix 센터가 이 timestamp 정보를 이용하여 복호화하므로 직접 선택 공격을 방지할 수 있다. 결국 이러한 공격들은 새로운 제안 방식에서는 성공할 수가 없게 된다.

다음으로 Shuffle형 익명 통신로에 적용한 Pfitzmann의 공격[6]을 제안 방식에 대한 공격 방법으로 고려할 수 있다. 결론적으로 새로운 방안은 잉여 정보 사용이나 안전한 bit commitment 방식을 사용함으로써 이러한 공격을 저지할 수가 있다. 이를 자세히 설명하면, Shuffle형 익명 통신로는 각 송신자가 보내는 암호문에 보내고자 하는 메세지 m_i를 평문 형태로 보내기 때문에 공격이 가능할 수 있었다. 즉 결과적으로, m_j''와 m_i의 대응 관계가 다른 출력들의 u승으로 쉽게 발견될 수 있었으며, 그리고 포멧이 정확한 다른 메세지로 바꾸어 최종적으로 출력될 수 있었다. 이러한 공격은 새로운 제안 방식에도 그대로 적용할 수 있다. 그러나 제안 방식에서는, 부정한 마지막 Mix 센터가 $\hat{\beta}_j / (Z_1 \cdots Z_k) = M_j'$를 만족하는 Z_k를 선택하여 M_j''를 M_j'로 바꾼다 할지라도, bit commitment 방식과 메세지에 첨부된 잉여 정보로 인하여 이러한 공격이 쉽게 검출될 수 있다. 이때 누가 부정한 행위를 하였는지를 찾아내기 위해서 영지식 상호 증명을 이용하면 부정자의 신원을 알 수 있으므로 그 부정자를 프로토콜상에서 제거한 후 프로토콜을 마지막까지 수행할 수 있다.

마지막으로 공격이 검출되고 공격자의 신분이 노출된다 할지라도 공격을 계속 시도하려는 경우에 대해서도 생각해 볼 수 있다. 이러한 시도는 제안된 방식에서는, 공격자들이 그 공격에서 오로지 암호문 밖에 알 수가 없으므로 쉽게 저지할 수 있다. 다시말해서 잉여 정보 테스트에서 오류가 발견될 경우는 다음 단계로 진행하지 않고 중지하기 때문이다. 결국 제안 방식은 Shuffle형 익명 통신로에 대한 Pfitzmann의 공격에 대해서 안전하며 우리들이 알고 있는 현재까지의 공격들에 대해서도 안전함을 알 수 있다. 또한 제안 방식은 Shuffle형 익명 통신로에서 사용했던 동시 동보 네트워크를 사용하지 않고도 구현할 수 있으므로 보다 실용적인 익명 통신로로써 사용될 수 있다.

7. 결 론

본 논문에서는 기존의 익명 통신로와 Shuffle형 익명 통신로에 대한 Pfitzmann의 공격을 검토하여 보고, 그 공격에 대해서 안전하고 실용적인 새로운 익명 통신로를 제안하였다. 제안 방식에 대한 여러 가지 공격은 bit commitment 방식이나 메세지에 첨부된 잉여 정보를 사용함으로써 쉽게 방지할 수 있다. 제안 방식에서는 각 송신자가 보내야 하는 암호문의 크기가 Shuffle형 익명 통신로보다는 다소 증가할지라도 Mix 센터의 수에는 전혀 의존하지 않고 일정하게 된다. 더우기, Shuffle형 익명 통신로에서 필요로 했던 동시 동보 네트워크는, 본 제안 방식에서는 더 이상 사용되지 않으므로 보다 안전하고 실용적인 익명 통신로로써 사용 가능하다.

참 고 문 헌

[1] T. ElGamal, "A public key cryptosystem and signature scheme based on discrete logarithms" *IEEE Trans. Inform. Theory*, Vol.31, No.4, pp.469-472, 1985.

[2] R. L. Rivest, A. Shamir, and L. Adleman, "A method for obtaining digital signatures and public-key cryptosystems", *Communications of the Association for Computing Machinery*, Vol.21, No.2, pp.120-126, 1978.

[3] D.L. Chaum, "Untraceble Electronic Mail, Return Addresses, and Digital Pseudonyms"', *Communications of the ACM*, Vol.24, No.2, pp.84-88, 1981.

[4] D.L. Chaum, "The Dining Cryptographers Problem: Unconditional Sender and Recipient Untraceability", *Journal of Cryptology*, Vol.1, No.1, pp.65-75, 1988.

[5] B.Pfitzmann and A.Pfitzmann, "How to break the direct RSA implementation of MIXes", *Advances in Cryptology, Proceedings of Eurocrypt'89*, pp.373-381, 1989.

[6] B.Pfitzmann, "Breaking an efficient anonymous channels", *Advances in Cryptology, Proceedings of Eurocrypt'94*, pp.332-340, 1994.

[7] C.S. Park, K.Itoh and K.Kurosawa, "Efficient Anonymous Channel and All / Nothing Election Scheme", *Advances in Cryptology, Proceedings of Eurocrypt'93*, pp.248-259, 1993.

[8] C.Rackoff and D.R.Simon, "Cryptographic Defense Against Traffic Analysis", *Proceedings of 25th ACM Symposium on Theory of Computing*, pp.672-681, 1993.

[9] M.Waidner and B.Pfitzmann, "The Dining Cryptographers in the Disco: Unconditional Sender and Recipient Untraceability with Computationally Secure Serviceability", *Advances in Cryptology, Proceedings of Eurocrypt'89*, pp.690, 1990.

[10] J.Bos and B. den Boer, "Detection of Disrupters in the DC Protocol", *Advances in Cryptology, Proceedings of Eurocrypt'89*, pp.320-327, 1990.

[11] M.Waidner, "Unconditional Sender and Receipient Untraceability in spite of Active Attacks", *Advances in Cryptology, Proceedings of Eurocrypt'89*, pp.302-319, 1990.

[12] A.Pfitzmann and M. Waidner, "Networks without user observability - design options", *Advances in Cryptology, Proceedings of Eurocrypt'85*, pp.245-253, 1986.

□ 著者紹介

박 춘 식(정회원)

광운대학교 전자통신공학과 졸업(학사)
한양대학교 대학원 전자통신공학과 졸업(석사)
일본 동경공업대학 전기전자공학과 졸업(암호학 전공, 공학박사)
1989년 10월 ~ 1990년 9월 일본 동경공업대학 객원 연구원
1982년 ~ 현재 한국전자통신연구소 책임연구원

※ 주관심 분야 : 암호이론, 정보이론, 통신이론