SCIS 2015 The 32nd Symposium on Cryptography and Information Security
Kokura, Japan, Jan. 20- 23, 2015
The Institute of Electronics, Information and Communication Engineers

属性に基づく認証鍵交換方式
Attribute based authenticate key exchange scheme

小林 鉄太郎* 星野 文学* 鈴木 幸太郎*
Tetsutaro Kobayashi Fumitaka Hoshino Koutarou Suzuki

あらまし インターネットで通信を行う際に、認証と鍵交換を行う SSL/TLS などのプロトコルが多く使われている。 従来の認証鍵交換プロトコルは、通信相手を指定してその相手とのみ鍵共有を行うものであった。 これを拡張し、通信相手の条件を指定して条件を満たす相手と鍵共有を行う方式を提案する。従来の ID ベース認証鍵交換方式と同様の eCK 安全性に加え、鍵共有相手の ID に関する情報を得ることがないという匿名性についての議論を行う。

キーワード 属性ベース暗号、認証鍵交換、匿名性

1 はじめに

インターネットで通信を行う際に、認証と鍵交換を行うSSL/TLSなどのプロトコルが多く使われている。 従来の認証鍵交換プロトコルは、通信相手を指定してその相手とのみ鍵共有を行うものであった。すなわち、通信を始める段階で通信相手の ID または公開鍵がお互いにわかっている状況を想定している。本論文では、相手の ID がわからない場合の通信を想定し、相手の条件を指定して条件を満たす相手と鍵共有を行う方式を提案する。ID ベース認証鍵交換と同様の方法で eCK 安全性を定義し、共有相手の ID に関する情報を得ることがないという匿名性についての議論を行う。

2 従来法

ID ベース認証鍵共有方式は、[1]などいくつか方式があるが、基本的にはAとBがお互いに相手のID情報ID_B、ID_Aを持っている状態で、乱数 x_A, x_B を生成し、$X_A=g^{xA}$ と $X_B=g^{xB}$ を交換し、ID_A、ID_Bに基づく固定秘密鍵 D_A, D_B を用いて共有鍵 K を計算する。

これを拡張した属性ベース認証鍵共有方式もすでに提案されている[2]が、安全性に関しては ID ベース認証鍵共有方式に準じており、匿名性の議論は行っていない。

* NTT セキュアプラットフォーム研究所, 〒１８０－８５８５, NTT Secure Platform Laboratories, 3-9-11, Midori-cho, Musashino-shi, Tokyo 180-8585 Japan, kobayashi.tetsutaro@lab.ntt.co.jp

3 安全性

本論文では、攻撃者が共有鍵に関する情報を得ることができない「eCK 安全性」と、通信プロトコルに参加するAとBが相手の ID に関する情報を得ることができない「匿名性」の定義を行う。

・eCK 安全性

米山ら[2] により提案された、属性ベース認証鍵交換に対する eCK 安全性の定義を属性ベースに拡張したものを示す。ID ベース eCK 安全性は、LaMacchia ら[3]による eCK 安全性を、ID ベースに拡張したものである。

定義１（安全性） 属性ベース認証鍵交換プロトコルΠに対する攻撃ゲームにおける攻撃者 A のアドバンテージを次のように定義する。

$$\mathrm{ADV}_{\Pi}^{\mathrm{AB\text{-}AKE}}(A) = \Pr[A.wins] - 1/2.$$

次の条件が満たされたとき、Π は属性ベース eCK モデルにおいて安全な ID ベース認証鍵交換という。

1. もし 2 人の honest なユーザが completed な matching session を実行したならば、セキュリティパラメータ に対して無視出来る確率を除いて両者は同じ session key を計算する。

2. 任意の確率的多項式時間攻撃者 A について、セキュリティパラメータに対して$\mathrm{Adv}^{\mathrm{AB\text{-}AKE}}(A)$が無視出来る。

[1][2]の方式はeCK-modelの安全性が満たされている。

・匿名性
以下の定義を満たす方式は匿名性を持つ。
定義２（匿名性）
通信相手のIDに関する情報を知ることができる確率が無視できる。

[1]の方式はIDベース方式であり、相手のID情報を持っている状態が前提であるため、匿名性を持っていない。[2]の方式についても匿名性については述べていない。

4　提案法

以下の関数を持つ属性ベース暗号を利用する。
KeyGen: 属性 Attr の入力に対し、属性秘密鍵鍵 D を出力する。
Enc: 条件 Poly と平文 M の入力に対し、暗号文 C を出力する。
Dec: 属性鍵 D と暗号文 C の入力に対し、平文 M を出力する。
属性ベース暗号と DH 鍵共有を組み合わせることで、eCK 安全性と匿名性を持つ方式を作ることができる。

・鍵生成
鍵発行局は、端末 A、B に対し、それぞれの属性 $Attr_A$,$Attr_B$ に応じた属性秘密鍵 D_A と D_B を生成し、配布する。

・鍵共有
端末Aは乱数 R_A' を生成し、R_A=Hash(R_A',D_A)を求める。X_A = g^R_A を求めてから暗号文 C_A = Enc($Poly_B$,X_A) を作成し、匿名公開掲示板に送信する。
同様に端末Bは乱数 R_B' を生成し、R_B=Hash(R_B',D_B) を求める。X_B = g^R_B を求めてから暗号文 C_B = Enc($Poly_A$,X_B) を作成し、匿名公開掲示板に送信する。
端末AとBは、それぞれ 暗号文 C_B と C_A を匿名公開掲示板から受信し、
端末 A は、復号演算 X_B'= Dec(D_A,C_B) を行い、K=X_B'^R_A を求める。
端末 B は、復号演算 X_A'= Dec(D_B,C_A) を行い、K=X_A'^R_B を求める。
端末AとBは、相手を特定せずに、かつ直接の通信を行わず、指定した条件 $Poly_A$ と $Poly_B$ が、それぞれ相手の属性 $Attr_A$, $Attr_B$ に当てはまる場合のみ、共有鍵 K を共有することができる。

5　安全性

・eCK 安全性
提案した属性ベース認証鍵交換方式は、DDH 仮定、属性ベース暗号が IND-CCA であること、Hash がランダムオラクルであることを仮定すれば eCK 安全である。

・匿名性
4 章で提案したプロトコルでは、端末 A と B が公開鍵掲示板に対して送信する情報は、属性ベース暗号の暗号文 C_A と C_B だけである。したがって、属性に関して漏えいする情報は属性ベース暗号の匿名性に依存する。匿名性を持つ属性ベース暗号[4]を用いれば、提案プロトコルも匿名性があることになる。

6　まとめ

属性に基づく認証鍵交換方式を提案した。ID ベース認証鍵交換方式における eCK 安全性に加え、匿名性の定義を行った。提案方式は eCK 安全と匿名性の両方を満たす。
提案方式は相手を特定せず、匿名公開掲示板を通じて鍵共有を行うため、1 対 1 の鍵共有にとどまらず、1 対 n の鍵共有を行うことができるが、その場合の安全性の検討については今後の課題とする。

参考文献

[1] Atsushi Fujioka, Fumitaka Hoshino, Tetsutaro Kobayashi, Koutarou Suzuki, Berkant Ustaoglu, and KzukiYoneyama, “ id-eCK Secure ID-Based Authenticated Key Exchange on Symmetric and Asymmetric Pairing,” IEICE Trans, Fundamentals, Vol. E96-A, No.6 JUNE 2013.
[2] Kazuki Yoneyama, “Strongly Secure Two-Pass Attribute-Based Authenticated Key Exchange, ” Pairing 2010: 147-166.
[3] B. LaMacchia, K. Lauter, and A. Mityagin, “Stronger security of authenticated key exchange,” ProvSec 2007, LNCS 4784: 1–16.
[4] Tatsuaki Okamoto, Katsuyuki Takashima, “Adaptively Attribute-Hiding (Hierarchical) Inner Product Encryption,” EUROCRYPT 2012: 591-608