鍵交換：現代暗号の誕生とその発展

Key Exchange : Advent of Modern Cryptography and Its Advance

岡本龍明 Tatsuaki OKAMOTO

アブストラクト 盗聴されてもいい通信路を使って二つの参加者が安全に鍵を交換（共有）するための方法は「鍵交換」と呼ばれ、その研究から現代暗号が誕生した。本稿では、歴史上最初に発表された「鍵交換」である Diffie-Hellman-Merkle (DHM) 鍵交換方式がどのように発展し、現代暗号理論の最先端においてどのように研究されているかを概観する。
キーワード 暗号、鍵交換、鍵共有、はん用的結合可能性、安全性証明

1. はじめに

1974 年、カリフォルニア大学バークレー校の修士課程の大学院生であった Ralph Merkle は、指導教授の理解のない状態で孤立しながらも、一つの画期的なアイデアに到達した。それは、盗聴されてもいい通信路を使って二つの参加者が安全に鍵を交換（共有）する方法（図 1）についてのアイデアであった。

この問題の重要性は今では広く認知されているが、当時はごくわずか（Merkle, Hellman, Diffie を含めた数人）の人にしか認識されていなかった。この問題は、今日では、鍵交換（KE:Key Exchange）もしくは鍵共有（KA:Key agreement）問題として知られ、また Merkle の発見したアイデアは、Merkle's puzzles と呼ばれて、歴史上初の鍵交換方式として知られている（その安全性レベルは低い）。Merkle が、その画期的なアイデアを論文として ACM の論文誌に投稿したのは、発見と同じ年の 1974 年であったが、その論文がその論文誌に掲載されたのは、

図 1 鍵交換 (KE:Key Exchange) 問題

なんと 4 年後の 1978 年であった⁽¹⁾。もし、この論文が、速やかに（例えば、1975 年に）掲載されていれば、現代暗号の歴史は、多少違っていただかもしれない（IEICE の論文査読者は、このようなことがないように、注意しましょう）。

Merkle の発見を 1974 年の段階で知っていた Hellman と Diffie は、その後研究を進め、ついに 1976 年、今日 Diffie-Hellman (DH) 鍵交換方式と呼ばれている方式を発見する。彼らは、このアイデアと公開鍵暗号及びデジタル署名の概念とあわせた論文を IEEE の論文誌に投稿した。この論文は、迅速に（投稿と同じ年に）1976 年に掲載され、現代暗号の誕生を告げる歴史的論文となる⁽²⁾。

このような経緯により、多くの人は、Merkle の貢献を忘れがちであるが、事情を熟知している Hellman だけは、いつも DH 鍵交換方式を Diffie-Hellman-Merkle (DHM) 鍵交換方式と呼んでいる。そこで、本稿でも、Hellman に倣って、DHM 鍵交換方式と呼ぶことにしよう。

本稿では、DHM 鍵交換方式の発見以来 30 年余りを経た現在、DHM 鍵交換方式を取り巻く最新の研究動向がどのようになっているかを見てみたい。

2. DHM 鍵交換方式

まず、DHM 鍵交換方式を紹介しよう。

この鍵交換方式により、離散対数問題という整数論の問題が暗号で初めて用いられた。離散対数問題とは、ある群 G （例えば、有限体の乗法群や有限体上定義された楕円曲線の群）の上で定義される。本稿では、群演算を乗法で表現する。群 G の離散対数問題とは、 g を位数が素数 p であるような G の要素、 $y = g^x$ （ここで、 $x \in \{0, 1, \dots, p-1\}$ ）としたとき、 (g, y, p) が与えられて、 x を求める問題のことである。一般に、群が十分に大きなサイズを持てば、離散対数問題を解くことは大変難しいとされている（これを「離散対数仮定」と呼ぶ）。なお、以降、 $\{0, 1, \dots, p-1\}$ を $\mathbb{Z}_p$ で表現する。

岡本龍明 正員：フェロー 日本電信電話株式会社 NTT 情報流通プラットフォーム研究所
E-mail tatsuaki.okamoto@lab.ntt.co.jp
Tatsuaki OKAMOTO, Fellow (NTT Information Sharing Platform Laboratories, Nippon Telegraph and Telephone Corporation, Musashino-shi, 180-8585 Japan).
Fundamentals Review Vol.1 No.4 pp.70-76 2008 年 4 月

DHM 鍵交換方式においては、群 G 及び位数が素数 p である G の要素 g がシステム共通のパラメータとして、全参加者に共有されているとする。

今、鍵交換を行う二人の参加者を Alice と Bob とする。まず、Alice は、ランダムに $x \in \mathbb{Z}_p$ を選び、 $A = g^x$ を計算し、Bob に送る。一方、Bob は、ランダムに $y \in \mathbb{Z}_p$ を選び、 $B = g^y$ を計算し、Alice に送る。Alice は、Bob との共有鍵 K として、 $K_A = B^x$ を計算し、Bob は、 $K_B = A^y$ を計算する (図 2)。

このとき、 $K_A = (g^y)^x = g^{xy} = (g^x)^y = K_B$ となるので、Alice と Bob は、鍵を交換 (共有) できる。一方、この通信を盗聴していた人は、 g^x と g^y を入手できるが、それらから交換された鍵である g^{xy} を計算することは、離散対数を解く (つまり、 g^x や g^y から x や y を求める) ことと同様に困難であると予想されている。この予想は、「Diffie-Hellman (DH) 仮定」と呼ばれている。

DHM 鍵交換方式は、DH 仮定が正しければ、受動的な攻撃 (盗聴をするだけの攻撃) に対しては安全であるが、次のような能動的な攻撃に対しては安全でないことが知られている。

今、Alice と Bob の通信路の中間にいて通信に能動的に関与する敵 Matt を考える。Matt は、図 3 に示すように、Alice との間では、 K_A という鍵を共有し、Bob との間では、 K_B という鍵を共有する。Alice と Bob は、お互いに正しい相手と鍵交換したと信じているため、Alice は鍵 K_A を用いて Bob に対して暗号通信を行い、Bob は鍵 K_B を用いて Alice に対して暗号通信を行う。一方、Matt は、Alice の Bob への暗号文は、鍵 K_A を用いて復号し、その復号した平文を鍵 K_B を用いて暗号化して、その暗号文を Bob に送る。Bob の Alice への暗号文も同様に処理する。このようにすると、Alice と Bob は、何の支障もなく通信ができるが、その通信内容はすべて Matt に盗聴されていることになる。

このような能動的な攻撃は「中間者 (MIM: Man-In-the-Middle) 攻撃」と呼ばれている。上記の例で分かるように、DHM 鍵交換方式は中間者攻撃に対しては安全でない。

それでは、どのようにすれば、このような中間者攻撃を防ぐことができるだろうか？ 上記の中間者攻撃が可能となった原因が、通信している相手が Bob なのか Matt なのかを Alice が確認しないまま、Bob と決め付けて暗号通信を行ったことにあるので、すぐに思いつく対策が、通信相手の認証を行うことである。このように、何らかの手段で通信相手の認証を行う鍵交換を「認証鍵交換 (AKE: Authenticated Key Exchange)」と

呼ぶ。

3. 認証鍵交換 (AKE)

認証鍵交換 (AKE) として、以下の二つの方式が活発に研究されてきた。一つは、認証として公開鍵インフラストラクチャ (PKI) を利用する鍵交換 (PKI ベース AKE) であり、もう一つが、認証としてパスワードを用いる鍵交換 (パスワード AKE) である。それ以外にも、ID ベース暗号・認証を用いた ID ベース AKE など様々な方式が活発に研究されている。

PKI は、現在、電子署名法などの法的制度も整備され、社会的インフラストラクチャとして定着しつつある。PKI では、認証機関 (CA) と呼ばれる (認定された) 機関が、各利用者の本人性・正当性を何らかの方法で確認した後、その公開鍵に対して (電子的な) 証明書を発行する。これは、各利用者の印鑑に対して役所が印鑑証明を発行することに対応している。

本稿では焦点を絞って、PKI ベース AKE に限定して紹介しよう。

3.1 デジタル署名を用いた AKE

まず最初に、認証としてデジタル署名を用いた PKI ベース AKE として、ISO で標準化されている方式 (ISO 9798-3) を紹介しよう (図 4) ³⁾。

まず、各参加者 (Alice と Bob) は、システムで定められた署名方式の鍵生成処理を個別に行い、その公開鍵 (署名検証鍵) を PKI の手順に従って登録処理を行う。ここでは、Alice の公開鍵 (公開検証関数) は Ver_A 、Bob の公開鍵は Ver_B とする (なお、ここで、 Sig_A 及び Sig_B は、Alice と Bob の秘密鍵 (秘密署名作成関数) とする。) 各参加者は何らかの手段で他の参加者の公開鍵を認証された形で受け取る。例えば、鍵交換プロトコルの中で、自分の公開鍵を認証局の証明書付きで相手に送ってもよい。

さて、鍵交換プロトコルの手順においては、Alice は、ランダムに $x \in \mathbb{Z}_p$ を選び、 $A = g^x$ を計算し、Bob に送る。Bob は、ランダムに $y \in \mathbb{Z}_p$ を選び、 $B = g^y$ 及び署名 $Sig_B(g^x, g^y, Alice)$ を計算するとともに、これらの情報を Alice に送る。Alice は、受け取った署名 $Sig_B(g^x, g^y, Alice)$ の検証を行い、正しければ Bob との共有鍵 K として、 $K_A = B^x$ を計算するととも

図 4 デジタル署名を用いた 3 交信 AKE

図 5 MQV 鍵交換方式

に, $\text{Sig}_A(g^y, g^x, Bob)$ を計算し Bob に送る. Bob は, 署名 $\text{Sig}_A(g^y, g^x, Bob)$ の検証を行い正しければ Alice との共有鍵 K として, $K_B = A^y$ を計算する.

なお, ここで, Alice 及び Bob の用いた x 及び y は, この鍵 K の生成のみに一時的に使われる使い捨ての情報であり, 鍵 K が交換された後は, ただちにそれぞれのメモリーから削除される. 従って, このプロトコルでは, 長期に保存する秘密鍵 (固定秘密鍵) Sig_A 及び Sig_B と使い捨ての秘密鍵 (一時秘密鍵) x 及び y という 2 種類の秘密鍵を用いている.

この方式の安全性については, 後に述べる.

4. MQV 鍵交換方式

上で紹介した署名を用いた AKE 方式は, 安全性の高い方式で, 実用的にも十分に効率的であるが, 3 回の交信が必要であること及び署名という別のプリミティブを必要とする点で効率の改善の余地がある.

そこで, 2 回の交信でかつ署名など他のプリミティブを用いないより効率の優れた方式が提案されている. そのような方式として, IEEE などで標準化されている Menezes-Qu-Vanstone (MQV) 方式を紹介しよう (図 5)⁴⁾.

このプロトコルにおいても, 上記の署名を用いた AKE 方式と同様に, 長期に保存する秘密鍵 (固定秘密鍵) と使い捨ての秘密鍵 (一時秘密鍵) という 2 種類の秘密鍵を用いる.

まず, Alice と Bob は, それぞれ固定秘密鍵として $a \in \mathbb{Z}_p$ と $b \in \mathbb{Z}_p$ をランダムに選び, 秘密に保存する. また, $A = g^a$ 及び $B = g^b$ を計算し, それぞれ A と B を公開鍵として PKI の仕組みで登録する (公開鍵の証明書を発行してもらう).

鍵交換プロトコルは, 基本的な DHM 鍵交換と同じであるが, 共有鍵の生成方法が異なる. Alice は, ランダムに $x \in \mathbb{Z}_p$ を選び, $X = g^x$ を計算し, Bob に送る. Bob は, ランダムに $y \in \mathbb{Z}_p$ を選び, $Y = g^y$ を計算し Alice に送る.

Alice は, 受け取った Y が $\mathbb{G}$ の要素であることを確認した後, Y のビット表現の上位 $|p|$ ビットを e とする ($|p|$ は, p のビットサイズを意味する.) また, X のビット表現の上位 $|p|$ ビットを d とする. 次に, 秘密鍵 (a, x) を用いて, $\sigma_A = (YB^e)^{x+ad}$ を計算し, Bob との共有鍵 K_A として, $K_A = KDF(\sigma_A)$ を計算する. ここで, KDF は, σ_A を乱数に変換する関数 (KDF :

Key Derivation Function) である. 同様に, Bob は, 受け取った X が $\mathbb{G}$ の要素であることを確認した後, 秘密鍵 (b, y) を用いて, $\sigma_B = (XA^d)^{y+be}$ を計算し, Alice との共有鍵 K_B として, $K_B = KDF(\sigma_B)$ を計算する.

ここで, 鍵が正しく交換できる理由は, $\sigma_A = (YB^e)^{x+ad} = (g^{y+be})^{x+ad} = (XA^d)^{y+be} = \sigma_B$ が成立するからである.

MQV 方式は中間者攻撃など通常の攻撃に対して安全と思われるが, 後に述べるような形でその安全性を証明することはできていない. そこで, あるモデル及び仮定の下で, 安全性が証明された方式として MQV 方式を改良した HMQV (Hashed MQV) 方式が Krawczyk により提案されている⁵⁾.

5. HMQV 鍵交換方式

HMQV 方式を図 6 に示す. HMQV 方式が MQV 方式と違う点は, e, d と K の作り方である. HMQV 方式では, e, d と K の作成において (暗号的) ハッシュ関数 H を用いる. ハッシュ関数は, 暗号においては様々な目的で利用される一方向性関数で, 与えられたデータを圧縮して (場合によっては, 伸張することもある) かく乱する関数であり, 米国標準局 (NIST) により定められた SHA-1, SHA-2 などが代表例である.

ハッシュ関数を用いる利点は, ハッシュ関数をランダム関数 (各入力に対する関数値をそれぞれ独立なランダムな値に設定し

図 6 HMQV 鍵交換方式

た関数)として理想化・仮定化してとらえて(これを「ランダムオラクルモデル」という),そのモデルの下では安全性の証明が容易になる点である。HMQV 鍵交換方式の安全性の定式化及びその結果については、後に述べるが、ランダムオラクルモデルの下で、安全性が証明される。

6. 認証鍵交換の安全性

さてそれでは、AKE の安全性がどのように定式化されてどのように証明されているかを紹介しよう。そのためには、まず現代暗号における安全性証明の現状を知る必要があるの、それから紹介しよう。

6.1 現代暗号の考える安全性

現代暗号の持つ大きな特徴が、非常に強い意味の安全性を考えるとということである。例えば、現代暗号では、暗号の安全性は単に暗号文から元のメッセージ全体が露呈しないという最も素朴な安全性のみならず、暗号文から元のメッセージの「いかなる部分情報」も露呈しないといった、より強い意味の安全性を持つことが求められるようになってきている。また、暗号文を解読しようとする攻撃のモデルも、攻撃者が単に通信文を受動的に盗聴するだけではなく、攻撃者が選んだ暗号文を復号し、それを攻撃者に教えるような状況を考慮するようになってきている。

暗号理論分野において、このような安全性を定式化する方法として、以下の二つのアプローチがある。

攻撃ベース定式化: 攻撃者とチャレンジャー間のゲームとして定式化するアプローチである。例えば、公開鍵暗号、デジタル署名など多くの暗号機能の安全性がこの方法で定式化されている。

シミュレーションベース定式化: 実際の方式(現実モデル)と、理想的な機能を使って現実をシミュレーションしたもの(理想モデル)との間のギャップが無視できるような場合に、この実際の方式が理想的な機能と同等の性質を持つととらえることにより、安全性を定式化する。このようなアプローチにより、暗号におけるすべての対象に対する統一的な安全性の定式化が可能とする。このようなアプローチの典型が、Canetti により提唱されたはん用的結合可能性(UC: Universal Composability)である。

なお、上記のような暗号理論分野において広く用いられているアプローチ(計算論的手法)のほかに、数理的技法(記号論理的証明手法)の立場からの安全性証明手法の研究も活発に行なわれている。本稿では、その分野との関連については紹介しないが、興味ある読者は文献(6)を参照されたい。

6.2 「認証鍵交換」の攻撃ベース定式化

Canetti と Krawczyk により、AKE の攻撃ベースの定式化が行われている⁽⁷⁾。ここでは、その定式化を CK 安全性と呼ぶ。

この定式化では、各参加者(Alice, Bob など)と敵(Matt)が対象となり、すべての参加者間の通信は Matt により支配されていると考える(つまり、Matt は、自由に盗聴、通信文の差し替え、廃棄などを自由にできる)。ここで、ある参加者が別の参加者と鍵交換のプロトコルを実行したとき、そのプロトコルの各参加者における入出力を「セッション」と呼ぶ(つまり、セッションは、各参加者ごとに定まる)。Alice と Bob が鍵交換のプロトコルを実行したときは、Alice のセッション sid_A と Bob のセッション sid_B が生じる。このとき、お互いに交信したセッション sid_A とセッション sid_B を「マッチングセッション」と呼ぶ。Alice と だれかが鍵交換プロトコルを実行し、Alice がその相手と鍵を交換できたと考えた鍵を Alice のセッション sid_A の「セッション鍵」 K_A と呼ぶ。

さて、Matt は、単に通信を支配するだけでなく、次の攻撃を許される。

セッション状態攻撃: ある参加者のセッションの状態(セッションをまたがる長期的な情報は含まれず、あくまでこのセッションだけに固有の情報)を Matt は知ることができる。

セッション鍵攻撃: あるセッションのセッション鍵を Matt は知ることができる。

参加者攻撃: ある参加者の持っているすべての情報を知ることができ、またその参加者の行動を支配できる。

次に、あるセッション sid が「攻撃されていない」かどうかを以下のように定義する。

- (1) セッション sid に関与するどちらの参加者も「参加者攻撃」を受けていない。
- (2) セッション sid が「セッション状態攻撃」もしくは「セッション鍵攻撃」を受けていない。
- (3) セッション sid のマッチングセッションが「セッション状態攻撃」もしくは「セッション鍵攻撃」を受けていない。

次に、敵 Matt は、ある「攻撃されていない」セッション sid を指定して、そこで次の二つのケースを区別できるかどうかのゲームを実行する。

- (1) そのセッション sid のセッション鍵 K_{sid} を Matt に与える。
 - (2) K_{sid} と同じサイズのランダムな鍵を Matt に与える。
- どのような敵 Matt も上の二つのケースを十分に区別できないとき、CK 安全であるという。

この CK 安全性が「中間者攻撃」に対処していることに注意されたい。中間者攻撃をする敵は、Alice と Bob とそれぞれに、別のセッションで通信しているため、それらはマッチングセッションにはならない。したがって、中間者攻撃で Bob との間のセッションでどのような攻撃をしても(しなくても)、Alice との間で鍵交換ができると、敵は上記の(1)と(2)のケースを区別できるので、上の CK 安全性に反することになる。

それでは、CK 安全性を満足する鍵交換方式はあるのだろうか? Krawczyk は、ハッシュ関数を理想化したランダムオラクルモデルにおいて、整数論的に妥当な仮定の下で、HMQV 鍵交換方式がこの安全性を満足することを示している。

6.3 シミュレーションベース定式化：はん用的結合可能性 (UC)

6.3.1 UC

現在、暗号機能は非常に広範に様々な形で使われている。例えば、暗号機能は様々な他の暗号（認証）機能と併用されることが多い。このとき、暗号機能単独で利用する場合には問題が生じないが、複数の暗号（認証）機能が相互に干渉し合っ、安全が損なわれるなど、利用状況において安全でない場合が起こるのである。

つまり、暗号機能がインターネット等における多くのアプリケーションで必須機能と認識され、広範に使われるようになればなるほど、「どのような環境で利用しても安全である」ことが要求されるようになるのである。

このような要求条件に答える安全性を非常に一般的な形で提示する概念が「はん用的結合可能性」(Universal Composability, 以下 UC と略すこともある)である⁽⁸⁾。

UC では、ある暗号機能を実行するプロトコルが理想的状況（理想的な機能を利用して実行）を模倣することができるならば安全と考える。例えば、ある公開鍵暗号方式が、理想的な公開鍵暗号機能をうまく模倣できることを示せば、その公開鍵暗号方式は理想的公開鍵暗号と同様の安全性を持つと考える。

まず、実現したい理想的機能 $\mathcal{F}$ を記述する。ここで、 $\mathcal{F}$ とはある暗号機能を実現するための理想的な信頼できるサービスとして記述する。例えば、暗号機能は、だれかに届けたい通信文を安全な通信路を使って正しく仲介するようなサービスとして記述され、署名機能は、ある利用者の文書を預かっておき、問い合わせがあれば、その利用者の文書であることを証明するようなサービスとして記述される。

次に、理想機能 $\mathcal{F}$ を使って暗号機能を理想的に実現した世界（理想世界）と現実の暗号方式／プロトコル π を実行する世界（現実世界）を区別する識別器（「環境」と呼ぶ）を導入し、どのような（確率的多項式時間チューリング機械である）環境 Z にとっても（もっと詳しく述べると、どのような現実世界の敵 A に対しても理想世界の敵 S が存在して、どのような環境 Z にとっても）、理想世界と現実世界を区別できないとき、 π は、理想機能 $\mathcal{F}$ を模倣できていると考える。つまり、暗号プロトコル π は $\mathcal{F}$ として記述された暗号機能を理想的な形で実現していると考えてよい。このことを、暗号プロトコル π は、理想機能 $\mathcal{F}$ を UC-実現すると呼ぶ。ここで、環境は、二つの世界を区別するために、各参加者と敵の入出力を対話的にコントロールすることができる（図7）。

この UC のフレームワークで最も重要な性質は名前の由来にもなっている、UC 定理（はん用的結合可能性定理）である。ここでは、UC 定理の記述は省略するが、大雑把にいうと、UC 定理が保証していることは、もし暗号プロトコル ρ が理想機能 $\mathcal{F}$ を UC-実現していることを示すことができれば、 ρ をどのようなプロトコルのサブルーチンとして利用しても、 ρ が $\mathcal{F}$ の機能を理想的に実現しているという性質が不変であるということである。

図7 UC 安全性の定式化

従来の安全性の定義ではこのような強い安全性は保証されていなかった。つまり、単独で使う場合には、目的とする機能（例えば、ゼロ知識証明）を満足していても、他のプロトコルと組み合わせると（もしくは、他のプロトコルの中で）使うと、本来の機能／安全性が保証されないことが起こり得たのである。例えば、二つのゼロ知識証明のプロトコルを並列に用いると、もはやゼロ知識証明ではない（知識を漏らす）ことが起こり得る。

6.3.2 UC に関する結果

上で述べたように、UC は、非常に強い意味の安全性を保証する。それでは、そのような UC 安全性を持つ方式をどのように構成すればよいであろうか？また、そのように強い安全性を持つ方式は現実存在するのであるか？その答えは、ある意味で否定的であるが、別の意味では肯定的である。

- (1) UC 公開鍵暗号の条件は、従来の標準的な安全性（選択暗号文攻撃に対して強秘匿／頑健）と同じである。また、UC 署名の条件も、従来の標準的な安全性（選択文書攻撃に対する存在的偽造不可）と同じである（肯定的結果）
- (2) 正しく動作する者が過半数の場合は、どのような多者暗号プロトコル機能も UC-実現可能（従来の、結果がそのまま使える。）（肯定的結果）
- (3) 正しく動作する者が過半数でない場合は、既存のいかなる多者暗号プロトコルも特に、多くの応用のある「二者暗号プロトコル」も UC-実現できない。例えば、多くの興味深い機能（コミットメント、ゼロ知識証明、コイン投げ等）が標準的モデル（プロトコルを実行する前に、いかなる事前処理も想定しないモデル）で UC-実現できない（否定的結果）
- (4) 共通参照情報（CRS: Common Reference String）モデル（プロトコルを実行する前に、ある仕様に基づく公開情報が第三者によって正しく作られ公開されることを想定するモデル）では任意の二者暗号プロトコル及び一般の多者暗号プロトコルが UC-実現可能である。つまり、共通参照情報モデルでは、UC コミットメントや UC ゼロ知識証明、UC 多者暗号プロトコルが実現可能である。（条件付肯定的結果）

6.3.3 「認証鍵交換」の UC による定式化

それでは、以上のような UC の定式化を鍵交換に適用するとどうなるだろうか？

図 8 に、利用者 A と B が、鍵配送機能 $\mathcal{F}_{KE}$ を用いて理想的に鍵配送を行う例を示そう。ここで、“exchange” は、理想機能に対する命令（コマンド）を意味し、sid は、各理想機能 $\mathcal{F}_{KE}$ の識別子である。UC においては、各 $\mathcal{F}_{KE}$ は、一つのサブルーチンコールに相当し、同一の機能でも、複数回（サブルーチンとして）利用されると、それぞれが別の識別子により認識される（つまり、複数の $\mathcal{F}_{KE}$ が生成される）。Adv は、敵を意味し、敵への通信を介入させている理由は、現実世界で敵が通信を妨害する状況と対応させるためである。いずれにしても、この理想的機能を用いた世界では、敵 Adv は、 A と B が共有した鍵 k に関する情報を一切得ることができないことに注目しよう。

ここで技術的に重要なことは、ある参加者が敵に攻撃されたときに理想機能の動作をどのように規定するかである。この規定により理想機能の保証する安全性のレベルが左右される。さて、ここではその詳細は省略するが、文献 (9) で規定された理想機能による UC 安全性は、前に述べた（ゲームベースの）CK 安全性よりも高い安全性を保証することが示されている。

なお、ここで注意する必要がある点は、一つの理想機能 $\mathcal{F}_{KE}$ は一つの sid にのみ対応しており、複数の sid にまたがった安全性は UC 定理で保証しているという点である。つまり、CK 安全性が複数のセッションを対象とした定式化であったことに対して、UC 安全性がそれとは顕著に異なる方法論で定式化していること、つまり「単一 sid の UC 安全性 + UC 定理」により複数セッションの UC 安全性を定式化していることに注意されたい。

さて、前に HMQV 鍵交換方式が CK 安全性を満足することを述べたが、この UC 安全性を満足するだろうか？ 答えは、否である。CK 安全性と UC 安全性の間にギャップがあるように具体的な鍵交換方式においても HMQV 鍵交換方式は CK 安全であるが UC 安全ではない。それでは、UC 安全性を満足する方式はどのような方式であろうか？ その答えは、前に紹介した署名鍵交換方式 (ISO 9798-3) である。これは、HMQV 鍵交換方式が 2 交信による方式であったのに対して、署名鍵交換方式が 3 交信であることが本質的に関与している。

図 8 「鍵交換」理想機能 $\mathcal{F}_{KE}$

それでは、2 交信鍵交換の安全性は CK 安全性で尽くされているだろうか？ その答えは、6.4 で述べる。

6.4 2 交信鍵配送方式の安全性

Krawczyk は、文献 (5) で、HMQV 方式の安全性を論じているが、CK 安全性以外にも幾つかの安全性を論じている。例えば、弱完全フォワード秘匿性 (wPFS: Weak Perfect Forward Secrecy)、鍵漏洩なりすまし安全性 (KCI: Resistance to Key-Compromise Impersonation Attacks) 及び一時秘密鍵漏洩安全性 (RLE: Resilience to the Leakage of Ephemeral Private Keys) などが (CK 安全性に含まれない安全性として)、文献 (5) で紹介されている。

ここで、wPFS とは、敵が対象とするセッション鍵 K の生成に能動的に関与していないという仮定の下で（いかなる参加者攻撃をしても）使い終わったセッション鍵 K を事後に知ることとはできないという安全性である。なお、完全フォワード秘匿性 (PFS) とは、敵が能動的に関与しても同様の安全性が保証されることを意味する。2 交信方式では、原理的に PFS は実現不可能であることが知られているので、wPFS が安全性要件となる。KCI は、Alice の固定秘密鍵が敵に漏えいしても、その敵は Alice に対して他の参加者 Bob になりすまして鍵交換ができないという安全性である（このとき、Alice になりすませることは明らかであるので、それは安全性要件とならない）。RLE は、Bob の一時秘密鍵が敵に漏えいしても、その敵は Alice に対して Bob になりすまして鍵共有ができないという安全性である。これら安全性が CK 安全性に含まれない理由は、CK 安全性における「攻撃されていないセッション」の定義が限定的であることによる。

いずれにせよ、HMQV 方式は、ランダムオラクルモデルの下で（及び数論的な仮定の下で）これらのすべての安全性を満足することが示されている。

しかし、このアプローチでは、CK 安全性を証明した後に wPFS, KCI, RLE などの安全性を個別に証明する必要があり、その証明はかなり煩雑かつ長大となる。従って、できれば何か統一的な定式化が欲しいところである。

最近、LaMacchia, Lauter, Mityagin がそのような目的で、2 交信鍵交換に特化して、CK 安全性及び wPFS, KCI, RLE などの安全性を包含するより安全の高い統一的な定式化を行っている（この安全性の定式化は、extended CK (eCK) 安全性と呼ばれている⁽¹⁰⁾）。また、実装に関する特殊な技法を用いることで、この安全性を満足する鍵交換方式が幾つか提案されている⁽¹⁰⁾⁻⁽¹²⁾（しかし、この実装に関する仮定の妥当性に関しては、議論があるところであろう）。

なお、文献 (10) で定義された eCK 安全性は、2 交信鍵交換に特化された定式化であり、より一般的な鍵交換（例えば 3 交信鍵交換）にはそのままでは適用できないこと、及び文献 (5) で記述されている CK 安全性も 2 交信鍵交換に特化されており、文献 (7) で示された一般的な CK 安全性とは必ずしも同一でないことに注意されたい。

7. ま と め

鍵交換そして DHM 鍵交換方式は、現代暗号誕生の源であり、そこから豊潤な現代暗号が開いた。驚くべきことに、その源である DHM 鍵交換方式そのものも、現在に至るまで発展し続け、現代暗号の中心的な課題として多彩な研究が進展している。本稿ではその一端を紹介した。本稿で紹介できなかったが、更にパスワードベース鍵交換やグループ鍵交換など、広はんな研究が行われている。この記事で現代暗号の面白さとその最先端の研究の雰囲気を感じて頂ければ幸いである。

岡本龍明（正員：フェロー）

1976 東大・工・計数卒。1978 同大学院修士課程了。同年 日本電信電話公社に入社。1989～1990 カナダ Waterloo 大客員助教授。1994～1995 米国 AT&T Bell Laboratories 客員研究員。本会業績賞、小林記念特別賞、電気通信普及財団賞、科学技術庁長官賞、日経 BP 賞各受賞。著書：「暗号・ゼロ知識証明・数論」（共立出版）、「現代暗号」（産業図書）、「暗号と情報セキュリティ」（日経 BP 社）など。現在、NTT 情報流通プラットフォーム研究所 岡本特別研究室長、NTT フェロー、京大大学院情報学研究科客員教授、2007 年度日本応用数学会会長。工博。現在、暗号理論の研究に従事。

文 献

- (1) R.C.Merkle, "Secure communications over insecure channels," Communi.ACM, vol.21,no.4, pp.294-299,1978.
- (2) W.Diffie,and M.Hellman," new directions in cryptography," IEEE Trans. Inf. Theor.vol.22, no.6, pp.644-654,1976.
- (3) ISO/IEC IS 9798-3, "Entity authentication mechanisms - Part 3: Entity authentication using asymmetric techniques," 1993.
- (4) L.Law,A.Menezes,M.Qu,J.Solinas,and S.Vanstone, "An efficient protocol for authenticated key agreement," Des. Codes Cryptogr., vol.28, no.pp.119-134,2003.
- (5) H.Krawczyk, "HMQV: A high-performance secure Diffie-Hellman protocol," Advances in Cryptology, CRYPTO 2005, LNCS 3621,pp2005, <http://eprint.iacr.org/2005/176>
- (6) 特集「数理的技法による情報セキュリティ」, 応用数理, vol.17, no.4, pp.6-58,2007.
- (7) R.Canetti,and H.Krawczyk, "Analysis of key-exchange protocols and their use for building secure channels," Advances in Cryptology, EUROCRYPT 2001, LNCS 2045,pp2001,<http://eprint.iacr.org/2001/040>
- (8) R. Canetti, "Universal composable security: A new paradigm for cryptographic protocols," FOCS'01.pp.136-145,2001. the full paper version, IACR Cryptology ePrint Archive, <http://www.iacr.org/2000/067>
- (9) R.Canetti,and H.Krawczyk, "Universally composable notions of key exchange and secure channel," Eurocrypt 02, (2002). Full version available at <http://eprint.iacr.org/2002/059>
- (10) B.LaMacchia,K.Lauter,and A.Mityagin, "Stronger security of authenticated key exchange," Cryptology ePrint Archive, Report 2006/073, 2006. <http://eprint.iacr.org/2006/073>
- (11) T.Okamoto, "Authenticated key exchange and Key encapsulation without random oracles," Cryptology ePrint Archive, Report 2007/473, 2007. <http://eprint.iacr.org/2007/473>
- (12) B.Ustaoglu, "Obtaining a secure and efficient key agreement protocol from (H)MQV and NAXOS," Cryptology ePrint Archive, Report 2007/123,2007. <http://eprint.iacr.org/2007/123>