7ZD-08

鍵生成局の不正な行為を考慮した 複数の鍵生成局を持つ ID ベース認証鍵交換の安全性モデル

割木 寿将 † 藤岡 淳 ‡ 永井 彰 § 安田 幹 ¶
神奈川大学大学院 † 神奈川大学 ‡ NTT 社会情報研究所 § NTT 社会情報研究所 ¶

1 はじめに

認証された session 鍵を二者間で秘密裏に共有できる暗号技術として，認証鍵交換があり，その一種に ID ベース認証鍵交換 (IBAKE: Identity-Based Authenticated Key Exchange) がある．

IBAKE ではユーザは ID 情報を公開情報として持ち，鍵生成局 (PKG: Private-Key Generator) という機関が ID 情報に対応した固定秘密鍵を生成する．IBAKE では公開鍵基盤を必要としないため，鍵長の観点から IBAKE を使用することが望ましい．

また，ユーザビリティの観点から同一の ID に対する固定秘密鍵を複数の PKG からもらうのが現実的であることから，複数の PKG が存在する IBAKE (mPKG-IBAKE: IBAKE with multiple PKGs) が提案されている．

しかし，mPKG-IBAKE の安全性モデルの一つである id(m)-aeCK モデル [1] では，全ての PKG が信頼できる機関として仮定されており，PKG の不正行為に対する安全性が考慮されていない．

本稿では PKG の不正な行為を考慮した mPKG-IBAKE の安全性モデルを二つ提案する．

Identity-Based Authenticated Key Exchange with Multiple Private Key Generators against Malicious Generators

† Kazuma Wariki, Kanagawa University
‡ Atsushi Fujioka, Kanagawa University
§ Akira Nagai, NTT Social Informatics Laboratories
¶ Kan Yasuda, NTT Social Informatics Laboratories

2 準備

2.1 id(m)-aeCK モデル

id(m)-aeCK モデル [1] では, PKG とは別に共通パラメータ生成局 (CPG: Common Parameter Generator) という機関が一つ存在し，マスタ公開鍵・秘密鍵 (msk_ι, mpk_ι) の生成時に必要な共通パラメータを $com \leftarrow \mathsf{ParGen}(1^\lambda; r_P)$ として生成している．ここで，λ はセキュリティパラメータ，r_P は乱数である．

また，それぞれの PKG は PID 情報を公開情報として持っており，msk_ι, mpk_ι の組を $(mpk_\iota, msk_\iota) \leftarrow \mathsf{MasKey}(com, PID_\iota; r_M)$ として生成する．ここで，r_M は乱数である．

このとき，攻撃者 $\mathcal{A}$ は以下のクエリを行うことができる．ここでは，PKG に関するクエリについてのみ述べる．

- $\mathsf{MasterKeyReveal}(PID_\iota)$: 指定した PKG のマスタ秘密鍵 msk_ι を得る．以降，MKR で記す．

安全性は，$\mathcal{A}$ と挑戦者 $\mathcal{C}$ の間のゲーム (experiment とよばれる) により定義され，$\mathcal{A}$ は $\mathcal{C}$ から com と $\{mpk_\iota\}$ が与えられる．そして，$\mathcal{A}$ には $\mathcal{C}$ から 1/2 の確率で session 鍵かランダムな鍵が与えられ，それがどちらであるかを判別できた場合，$\mathcal{A}$ の勝ちとする．さらに，mPKG-IBAKE 方式 Π に対する，$\mathcal{A}$ の優位性を以下のように定義し，これがすべての $\mathcal{A}$ に対し無視できる場合，Π は id(m)-aeCK 安全であるとする．

$$\mathbf{Adv}_{\Pi}^{\text{id(m)-aeCK}}(\mathcal{A}) = \Pr[\mathcal{A} \text{ の勝ち }] - \frac{1}{2}.$$

3 提案モデル

以下では，mPKG-IBAKE の新たな安全性モデルについて述べる．ただし，id(m)-aeCK モデルとの差分のみ述べる．

3.1 id(m)-aneCK モデル

PKG の不正行為を以下のクエリでモデル化する．

- RandomStringReveal(PID_ι): 指定した PKG が MasKey 実行時に使った乱数 r_M を得られる．

また，MKR は id(m)-aeCK モデルと同じとし，experiment，優位性は id(m)-aeCK モデルと同様に定義する．

3.2 id(m)-areCK モデル

PKG の不正行為を以下のクエリでモデル化する．

- ParameterReplace($mpk'_\iota||msk'_\iota$): $\mathcal{C}$ にメッセージ $mpk'_\iota||msk'_\iota$ を送り，mpk_ι を mpk'_ι に，msk_ι を msk'_ι に置き換えることを要求する．以降，PR で記す．

また，MKR は id(m)-aeCK モデルと同じとする．

experiment では，$\mathcal{A}$ は $\mathcal{C}$ から com と $\{mpk_\iota\}$ を受け取ったあと，PR を実行する．それ以降，PR 以外のクエリを任意に実行できる．また，優位性は id(m)-aeCK モデルと同様に定義する．

3.3 安全性モデルの強弱関係

以下の図 1 は，安全性モデル間の implication と separation を示している．implication に関しては，ほぼ自明なため記述を割愛する．

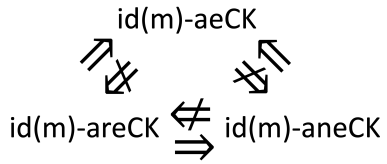

図 1 安全性モデルの強弱関係

id(m)-aeCK 安全 $\nRightarrow$ id(m)-aneCK 安全を示すために，藤岡が IWSEC2017 で提案した方式 [1] に対して，ISEC2020-12 で紹介した PKG に乱数消去を導入した手法 [2] を適用した方式 (以下，変形藤岡方式とよぶ) を用いて，この変形藤岡方式が以下の補題を満たすことを示す．

補題 1. 変形藤岡方式は，ランダムオラクルモデル下で，GBDH 仮定の元，id(m)-aeCK 安全を満たす．

補題 2. 変形藤岡方式は id(m)-aneCK 安全を満たさない．

また，id(m)-aneCK 安全 $\nRightarrow$ id(m)-areCK 安全を示すために，id(m)-aneCK 安全な方式を $mpk_\iota = mpk'_\iota$ の場合に session 鍵を固定する方式に変換する．この時，$mpk_\iota = mpk'_\iota$ となる確率は無視できるため，id(m)-aneCK 安全である．一方で id(m)-areCK モデルの $\mathcal{A}$ は PR により mpk_ι を mpk'_ι に置き換えることで容易に session 鍵を得られ, id(m)-areCK 安全が破れる．

図 1 から，id(m)-areCK モデルが最も強い安全性モデルであることがわかる．

4 まとめ

本稿では，鍵生成局の不正な行為を考慮した mPKG-IBAKE の安全性モデルとして，id(m)-aneCK モデルと id(m)-areCK モデルを提案した．また，id(m)-aeCK, id(m)-aneCK, id(m)-areCK モデルの関係を示した．

参考文献

[1] A. Fujioka. Adaptive security in identity-based authenticated key agreement with multiple private key generators. In *IWSEC2017*, pp. 192–211. Springer, 2017.

[2] 割木寿将, 藤岡淳, 佐々木太良, 鈴木幸太郎, 富田潤一. IoT 機器向け ID ベース認証鍵交換と不正な PKG に対する安全性. 信学技報 ISEC2020-12, 信学会, 2020.