Fujioka-Suzuki-Xagawa-Yoneyama の概要

国立研究開発法人 情報通信研究機構

1. 基本情報

- ✧ 名前

  Fujioka-Suzuki-Xagawa-Yoneyama (FSXY)

- ✧ 機能

  暗号として鍵カプセル化メカニズム (Key Encapsulation Mechanism, KEM) を用いた認証付き鍵交換プロトコルの一般的構成法。

- ✧ 関連する文書

  A.Fujioka, K.Suzuki, K.Xagawa, and K.Yoneyama, "Strongly secure authenticated key exchange from factoring, codes, and lattices," Cryptology ePrint Archive: Report 2012/211, http://eprint.iacr.org/2012/211.pdf.

2. プロトコル仕様

鍵カプセル化メカニズムは IND-CCA 安全とする。本文書では、2 パスの鍵交換のシーケンスを図 1 に示す。

3. 攻撃者モデル（自然言語による記述）

Krawczyk により提案された強い安全性モデル（CK+モデル）を想定している。

4. セキュリティ要件（自然言語による記述）

CK+モデルにおいて、エンティティ U_A とエンティティ U_B の共有するセッション鍵が、想定されていないエンティティに対して秘匿された上で、BS と SS の間で認証鍵 AK 及びセッション鍵 TEK を共有する。さらに、これらの鍵が攻撃者に秘匿される。

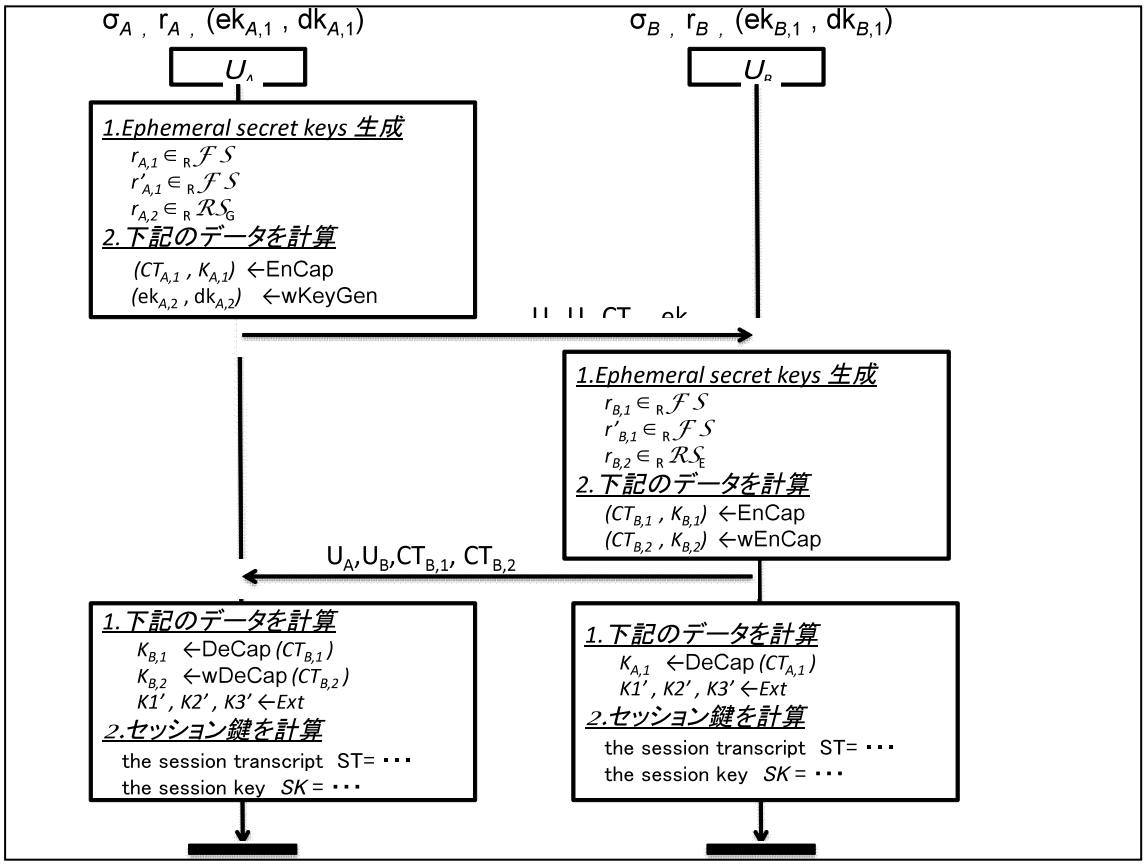

図 1. シーケンス図

5. 安全性に関して知られている結果

5.1. 脅威/脆弱性

特になし。

5.2. 形式手法に基づく検証

形式手法に基づく検証はなされていないが、関連する文書で安全性証明が示されている。

6. 備考

本文書は、**総務省「暗号・認証技術等を用いた安全な通信環境推進事業に関する実証実験の請負　成果報告書」**からの引用である。