ProVerif を用いた Bluetooth の安全性解析：Passkey Entry モードの検証に向けて

塚田研究室　218K6023　河合　悠斗

1　はじめに

暗号プロトコルの自動検証ツールとして ProVerif[1]がある。一方、Bluetooth は周辺機器を接続する際に用いられる無線通信方式である。端末間で相互認証し、関連付けを行う手順をセキュアシンプルペアリング（SSP）と呼ぶ。まず Chang ら[2]によって SSP のモードの１つである Numeric Comparison モードに対する攻撃法が、井上ら[3]によって Passkey Entry モードに対する攻撃法が発見された。Yeh ら[4]がこの Numeric Comparison モードの問題に対して改良案を提案している。しかし、横山らによる ProVerif を用いた安全検証により Yeh らの Numeric Comparison モードの攻撃法が確認され、その攻撃法に対する対策が行われた[5]。しかし一方、改良された Passkey Entry モードはあるが、安全検証が行われていない。

本研究では Yeh らの Numeric Comparison モードについて ProVerif を用いた安全性検証の再現実験を行う。さらに改良された Passkey Entry モードの検証に向けて形式化する上での難しさや予想される攻撃法について考察する。

2　ProVerif

ProVerif は Blanchet らが開発した形式モデル上での自動検証ツールであり、暗号プロトコルで要求される秘匿性や認証性などの安全性を検証可能である。ProVerif はさまざまな暗号プロトコルの検証に用いられ、多くの暗号プロトコルに対して脆弱性を発見することに成功している。

3　Bluetooth

3—1　Bluetooth の概要

Bluetooth の SSP には４種類のモードがある。Numeric Comparison モードではデバイス両方の画面に数字が表示され、一致確認し、認証を行う。Passkey Entry モードではマスター側で表示された６桁の数字（パスキー）をデバイス側に入力して認証を行う。

SSP は５つのフェーズからなる。フェーズ１では楕円曲線 Diffe Hellman(ECDH)鍵共有により公開鍵を交換し、共有鍵(DHkey)を生成する。フェーズ２ではフェーズ3､4で用いられる値を共有する(図1)。フェーズ３では共有した全ての値が端末間で正しく共有できていることを検証する。フェーズ４でリンクキーを生成し､フェーズ５で認証･暗号化を行う。フェーズ２では端末が持つユーザインターフェース I/O によってモードが選択される。

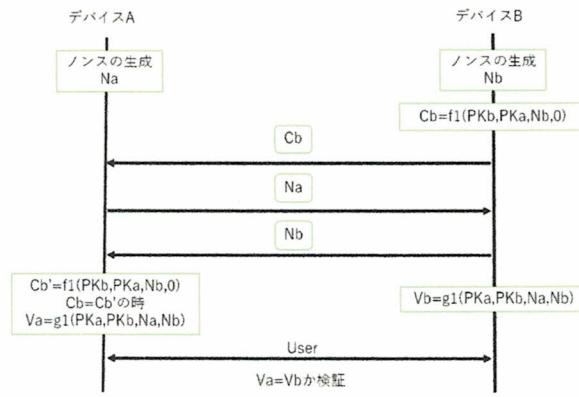

図 1. Numeric Comparison モード(フェーズ２)

3—2　Yeh らの Numeric Comparison モード

本節では Yeh らの Numeric Comparison モードについて説明する。Yeh らの Numeric Comparison モードは目視確認に伴う人為的ミスへ対策に加え、中間者攻撃に耐性を持つようにフェーズ１、２、３を組み合わせて改良された。

図２にしたがって Yeh らの Numeric Comparison モードを説明する。デバイス A､B ともに PIN の値を入力する。デバイス A は Bluetooth Device 値 A､I/O 情報 I/OcapA､PKa⊕PIN を送信する。デバイス B は受け取った値 PKa⊕PIN に対して PIN を排他的論理和し、デバイス A の公開鍵 PKa を得る。自身の秘密鍵 SKb と PKa から DHkey の生成を行う。デバイス B はハッシュ値 Cb を計算し、Cb、B、IOcapB、PKb⊕PIN を送信する。デバイス A は受け取った値 PKb⊕PIN に対して排他的論理和し､デバイスBの公開鍵PKbを得る。

SKa と PKb から DHkey の生成を行う。デバイス A は Cb’ を計算し、Cb=Cb’ を検証する。異なる時、ペアリングを中断し、等しい時、デバイス B に Ca を送信する。デバイス B は Ca’ を計算し、Ca=Ca’ を検証する。異なる時、デバイス B はペアリングを中断し、等しい時、フェーズ 4 に進む。リンクキーLK を計算し、この LK を用いて共有鍵 Kc を得る。

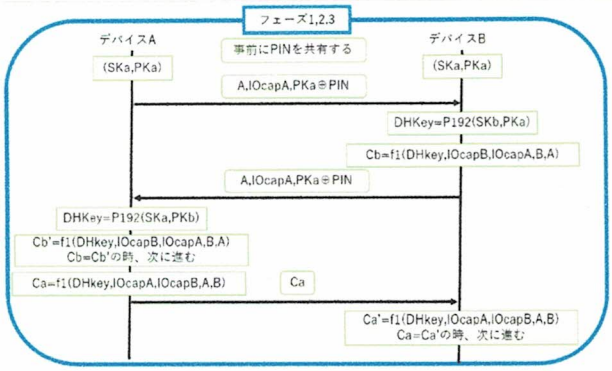

図 2. Yeh らの Numeric Comparison モード(改良部分)

4 検証結果

Yeh らの Numeric Comparison モードを ProVerif により形式化し、秘匿性、認証性について先行研究[5]と同様の検証を行った。

表 1. 認証性の検証結果

Property			Result
Strong Authentication	Injective	A-to-B	False
		B-to-A	False
	Non-injective	A-to-B	True
		B-to-A	False
Weak Authentication	Injective	A-to-B	False
		B-to-A	False
	Non-injective	A-to-B	True
		B-to-A	False

結果、秘匿性は、共有鍵 Kc が満たしていることを確認した。表 1 より認証性は、デバイス A によるデバイス B の認証の場合、Non- injective が成立している。ただし、Injective は成立していないため、再生攻撃を受ける。デバイス B によるデバイス A の認証の場合は Non-injective も Injective も成立していないため、なりすましが可能である。この結果は先行研究[5]で報告されている結果と一致した。

5 まとめ

Yeh らの Numeric Comparison モードを ProVerif で形式化し、安全性検証を行い、先行研究[5]と同様の結果を得られた。

Passkey Entry モードを形式化する上で考えられる難しさを説明する。Numeric Comparison モードと異なる点は、入力した 10 進数 6 桁の値(20bit)のノンスを 1bit ずつ計算に用いて、20 回繰り返す点であり、これが ProVerif で形式化する上で、難しいと考えられる。また、先行研究[3]よりなりすましへの攻撃法が確認されている。よってなりすましへの対策を講じていると考えられるが、Yeh らの Numeric Comparison モードのように一部だけ修正してもまだなりすましの可能性が排除できない。それに加え、再生攻撃も可能であるのではないかと予想される。

参考文献

[1] Bruno Blanchet：“ProVerif”，https://prosecco.gforge.inria.fr/personal/bblanche/proverif/

[2] R. Chang and V. shimatikov: Formal Analysis of Authentication in Bluetooth Device Paring, Proc. Joint Workshop on Foundations of Computer Security and Automated Reasoning for Security Protocol Analysis (FCS-ARSPA 2007), pp. 45-61 (2007)

[3] 井上 博之, 荒井 研一, 金子 敏信： “ProVerif による Bluetooth のセキュアシンプルペアリングに対する形式的な安全検証”，日本応用数理学会 2013 年春の研究部会連合発表会「数理的技法による情報セキュリティ」(FAIS)セッション, 2013

[4] T. C. Yeh, J. R. Peng, S. S. Wang, and J. P. Hsu：“Securing Bluetooth Communications”，International Journal of Network Security, Vol. 14, No. 4, pp. 229-235, July 2012

[5] 横山 雄太, 岩本 智裕, 荒井 研一, 金子 敏信：“ProVerif を用いた Bluetooth のセキュアシンプルペアリングの形式的検証”，Computer Security Symposium 20, 21-23 October 2013