バイブレーションを用いた机上のスマートデバイス間における秘密鍵生成手法

アーノ 有里紗† 豊田 健太郎†† 渡邊 裕治‡ 笹瀬 巌†††

† 慶應義塾大学
arno@sasase.ics.keio.ac.jp

†† 慶應義塾大学
toyoda@sasase.ics.keio.ac.jp

‡ 日本アイ・ビー・エム 東京基礎研究所
muew@jp.ibm.com

††† 慶應義塾大学
sasase@ics.keio.ac.jp

あらまし スマートフォンの近距離無線通信技術を用いた電子決済および端末間でのデータ共有アプリケーションにおいて中間者攻撃が問題となっている．この攻撃は攻撃者が無線信号を傍受し通信を行う端末と近接していると見せかけることで可能となるため，正規の端末が近接していることを証明する端末間での秘密鍵共有を行う技術が求められている．そこで本研究では秘密を共有したい端末を同一の机上に置き，ある端末にランダムなパターンで振動させ，他の端末は加速度を測定することで，各端末が測定した加速度を基に秘密鍵を生成する手法を提案する．Android 端末を用いて提案方式を実装し，本研究の有効性を示す．

Private Key Generation in Two Smart Devices on the Desk Using Vibration

Alisa Arno† Kentaroh Toyoda†† Yuji Watanabe‡ Sasase Iwao†††

†Keio University
arno@sasase.ics.keio.ac.jp

††Keio University
toyoda@sasase.ics.keio.ac.jp

‡IBM Research - Tokyo, IBM Japan Ltd.
muew@jp.ibm.com

†††Keio University
sasase@ics.keio.ac.jp

Abstract The man-in-the-middle attack is a real concern in mobile NFC (Near Filed Communication) payment applications and data sharing applications. We need a technique to share the private key to show whether two smart phones are close or not to prevent the man-in-the-middle attack. In this paper, we propose a non-interactive key sharing scheme with vibration and accelerometer. We put devices on a table and let a device vibrate with a random pattern and the devices measure it to extract a key from measured acceleration. We implement our scheme with Android smartphones to show the effectiveness of the proposed scheme.

1 はじめに

近年，スマートフォンおよびタブレット端末が急速に普及しており，それにともない NFC (近距離無線通信：Near Field Communication) を用いた電子決済サービスおよび端末間でのデータ共有アプリケーションが拡大している．しかし，NFC はデータ通信を行う端末間に攻撃者が入り込み，攻撃者が各正規の端末に対してデー

タの盗聴および改ざんを行う中間者攻撃に対して脆弱であることが指摘されている [1]．中間者攻撃を防ぐために，正規の端末が物理的に近接しているかによって正規の端末と攻撃者を判別する認証方式が挙げられる [3]．具体的には，端末間の通信遅延を測定することで端末間の物理的距離を推定する距離制約プロトコルが挙げられる．この方式では端末間の距離の推定を可能とする一方，通信遅延に非常に敏感という問題点がある．

そこで近年，スマートフォンで測定可能な環境情報である光，音，気温，温度，GPS などの周囲の環境情報を利用して端末の距離を測定する手法が検討されている [4–14]．しかしながら，端末が近接でないと得られない情報を利用可能という利点がある一方，環境情報は変化に乏しいことや位置情報に関するプライバシが守られないという問題がある．

本研究では秘密を共有したい端末を同一の机上に置き，それぞれの端末でランダムに生成したバイブレーションパターンで振動させ，各端末の加速度情報を観測することで，正規の端末間での秘密鍵生成手法を提案する．本提案方式ではユーザの特別の操作なしに，通信を行う端末で秘密鍵の生成可能にする．Android 端末を用いて提案手法を実装し, 特性評価を行い, 提案方式の有効性を示す．

以下 2 章では関連研究，3 章では提案方式について説明する．4 章では提案方式の有効性を示すため特性評価を行い，5 章でまとめを行う．最後に今後の課題について述べる．

2　関連研究

IoT (Internet of Things) デバイスのセンサを利用し，周囲の環境情報を基にした認証および秘密鍵共有方式および加速度情報を基にした方式についてまとめる．

T.Halevi 等は光情報および音情報を基に，正規のリーダとタグが近接しているかを判別する，安全な電子決済のための近接検知方式を提案している [4, 5]．この提案ではリーダとタグで測定された光および音情報を銀行に送り，銀行が送られてきた情報から電子決済を行うかの判断を下す．D.Ma 等は，HF 帯の RFID において，GPS を基にした位置認証で中間者攻撃を防止する方式を提案している [6]．タグは正規のリーダの位置情報のリストを所持し，タグがリストに載っているリーダに近接したときのみ，応答する．P.Urien 等はリーダおよびタグで測定した表面温度を共有鍵として認証を行う方式を提案している [7]．B.Shrestha 等は気温，湿度，排気ガス，標高の 4 つのセンサを利用して，2 つの通信機器が近接してるかの判別方式を提案している [9]．

光や音のセンサを用いた方式は，秘密共有のために無線通信を使用する必要がないという利点がある．一方で，具体的にどの程度近接していれば認証に成功かを判定することが困難である．例えば，光センサや音センサを用いて室内で認証を行う際に，同一の部屋に存在する攻撃者も同様の情報を取得できる可能性がある．また GPS を利用した方式においては，室内での利用が困難である．

そこで R.Mayrhofer 等は周囲の環境情報の代わりに加速度センサを利用する方式を提案している [13]．この方式では，通信を行う 2 つの端末を重ね合わせて振り，振っている間に測定した加速度が同一であるかどうかで認証を行う方式を提案している [13]．

この方式は，正規の端末間のみが観測しうる加速度を意図的に生成することで，周囲の環境情報に依存せず秘密共有を行うことを可能とする．一方で，端末を 2 台片手に持ち，振らなければならないため，タブレット端末での使用や，3 台以上で秘密共有を行う場合などに不適である．

3　提案方式

本研究では携帯端末同士で安全に通信を行うために，バイブレーションを使用した秘密鍵生成手法を提案する．この手法では 2 つの携帯端末は隣同士に机の上に置き，それぞれ異なったパターンで振動させ，そのときの加速度を両携帯端末で測定する．これによりワンタイム秘密鍵を生成可能であり，さらに端末の振動してい

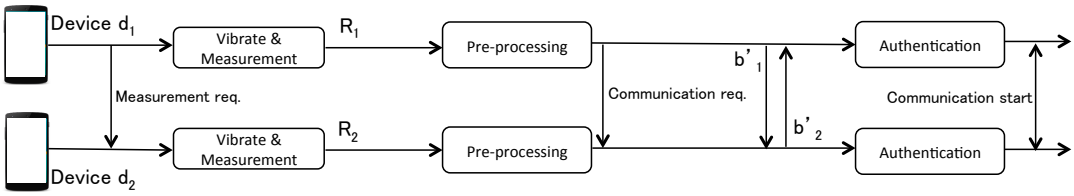


図 1: 提案方式

る様子を攻撃者が視覚的に認識するのは困難である．両携帯端末を同時に振動させたときに測定した加速度から，自身の端末の振動パターンの加速度を差し引くことにより，相手が単体で振動させたと予想される加速度を得ることができる．このとき，加速度センサの感度は非常に高いために測定した加速度に対して前処理を行う．最後に各端末で予想された加速度の平均値を閾値としてバイナリに変換し，変換された値を秘密鍵に使用する．

3.1 アルゴリズム

図 1 に提案方式の手法を示す．端末 d_1 および端末 d_2 は机の上に隣同士にあり，端末 d_1 は端末 d_2 にデータを送信したいとする．通信に必要な秘密鍵を生成するために端末 d_1 から端末 d_2 に Measurement req. を要求する．以下手法の各プロセスを説明する．

Vibration & Measurement: 端末 A から Measurement req. を送信した後，端末 d_1 と端末 d_2 で異なったバイブレーションパターン

$$\{t_{1,ON}, t_{1,OFF}, t_{2,ON}, t_{2,OFF}, \cdots\}$$

で振動させ，その加速度の測定を行う．$t_{i,ON}$ および $t_{i,OFF}$ はそれぞれ i 番目に振動させる時間および振動を休止する時間を表し，j は端末を示すインデックスとし，$j \in \{d_1, d_2\}$ とする．端末の加速度情報を端末に内蔵された加速度センサで測定する．ここで，端末は机上に置いてあるため重力は考慮しない．加速度センサは x 軸，y 軸，および z 軸それぞれの加速度情報を測定する．

Pre-processing: 端末で測定された加速度情報の軸は携帯端末座標軸であるため，式 (1)-(6) を用いてデカルト座標系に変換する．$a_{x,j,t}$，$a_{y,j,t}$，$a_{z,j,t}$ をそれぞれある t 秒のときに測定した携帯端末 j の座標 x 軸，y 軸，z 軸の加速度，$r_{j,t}$ を携帯端末座標軸から求めた 3 軸加速度ベクトル，$\theta_{j,t}$ および $\phi_{j,t}$ を偏角，$A_{x,j,t}$，$A_{y,j,t}$，$A_{z,j,t}$ をそれぞれデカルト座標系に変換した x 軸，y 軸，z 軸の加速度とする．

$$r_{j,t} = \sqrt{a_{x,j,t}^2 + a_{y,j,t}^2 + a_{z,j,t}^2}, \quad (1)$$

$$\theta_{j,t} = \arccos\left(\frac{a_{z,j,t}}{r_{j,t}}\right), \quad (2)$$

$$\phi_{j,t} = \arctan\left(\frac{a_{y,j,t}}{a_{x,j,t}}\right), \quad (3)$$

$$A_{x,j,t} = r_{j,t}\sin\theta_{j,t}\cos\phi_{j,t}, \quad (4)$$

$$A_{y,j,t} = r_{j,t}\sin\theta_{j,t}\sin\phi_{j,t}, \quad (5)$$

$$A_{z,j,t} = r_{j,t}\cos\theta_{j,t}. \quad (6)$$

加速度センサの感度は高いためノイズを除去する必要がある．文献 [3] に示された手法と用い，式 (7)-(9) を用いて $A_{x,j,t}$，$A_{y,j,t}$，および $A_{z,j,t}$ のノイズ除去を行う．$A'_{x,j,t}$，$A'_{y,j,t}$，および $A'_{z,j,t}$ をノイズ除去後の加速度とする．

$$A'_{x,j,t} = \frac{-3A_{x,j,t-1} + 2A_{x,j,t} + A_{x,j,t+1}}{4}, \quad (7)$$

$$A'_{y,j,t} = \frac{-3A_{y,j,t-1} + 2A_{y,j,t} + A_{y,j,t+1}}{4}, \quad (8)$$

$$A'_{z,j,t} = \frac{-3A_{z,j,t-1} + 2A_{z,j,t} + A_{z,j,t+1}}{4}. \quad (9)$$

加速度情報は，デカルト座標系に変換した加速度から求めた 3 軸加速度ベクトル $R_{j,t}$ であり，式 (10) として表される．

$$R_{j,t} = \sqrt{A'^2_{x,j,t} + A'^2_{y,j,t} + A'^2_{z,j,t}}. \quad (10)$$

ここで $R_j = \{R_{j,1}, R_{j,2}, \cdots, R_{j,T}\}$ とし，t は測定時間 $t \in [1, T]$ を表す．

Authentication：測定終了後，端末 d_1 はデータを送信したい端末 d_2 に Communiation req. を送信する．Communication req. を受信後，両端末で R_j から自身の振動パターンを算出した加速度情報 I_j を引くことにより．各端末で相手の端末の生成した振動パターンによる加速度情報 $R'_j = \{R'_{j,1}, \cdots R'_{j,T}\}$ を求める．

$$R'_{j,t} = \begin{cases} R_{j,t} - I_{j,t} & (R_{j,t} > I_{j,t}) \\ 0 & (otherwise). \end{cases} \quad (11)$$

携帯端末に内蔵されている加速度センサは 1 つであるので，R_j を測定しながら I_j を測定することはできない．しかし，各端末は自分がこれからどのようなパターンで振動させるのかを認識しているため，自分が振動させたときの加速度情報を予想することが可能である．$I_{t,j}$ において t_{OFF} のとき $0[m/s^2]$，t_{ON} のとき $5[m/s^2]$ を代入するとする．R'_1 および R'_2 の平均値 m_j を用いてバイナリデータに変換する．式 (12) を用いて加速度情報をビットに変換する．変換後のビット列 b'_j をそれぞれの端末の秘密鍵とする．

$$b'_{j,t} = \begin{cases} 1 & (R'_{j,t} > m_j) \\ 0 & (otherwise) \end{cases} \quad (12)$$

生成された秘密鍵 b'_1 を端末 d_2 に，秘密鍵 b'_2 を端末 d_1 に送信する．ここで I_j に足しても式 (12) と同様にバイナリデータに変換する．I_1 をビット変換したものを b_1，I_2 をビット変換したものを b_2 とする．端末 d_1 で b_1 および b'_2 を，端末 d_2 で b_2 および b'_1 の比較を行い，一致率が閾値以上になったときに認証を行う．

4　特性評価

提案方式の有効性を示すために，スマートフォンを用いた実証実験を行う．図 2 に実験環境を示す．提案方式では，2 台の Android 端末の Nexus 5 を端末 d_1 および端末 d_2 として用い，それらを木製の机上に配置し，実験を行った．また本提案方式の加速度は 0.02[sec] 間隔で測定した．これはサンプリング間隔が短すぎると加速度情報にノイズが入りやすく，長すぎると正確

図 2: 実験環境

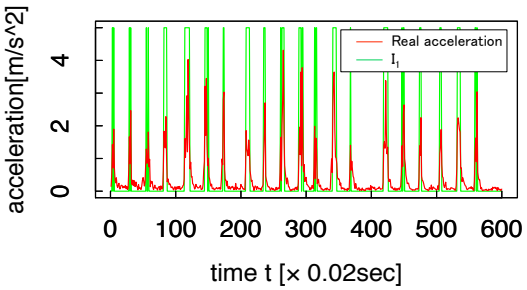


図 3: 自身の振動パターンから予測した加速度情報と実際に単体のみで振動させたときに測定した加速度

な加速度を測定することができないと判断したためである．まず初めに，式 (12) において，自身の振動パターンから予測した加速度情報と，実際にそのパターンを振動させ，自分自身で観測した加速度情報がどの程度一致するのかを検証する．図 3 にその結果を示す．図 3 から I_j は各端末のみで振動させた加速度と言える．

4.1　相手の波形の予測

図 4 に両端末を同時に異なったバイブレーションパターンで振動させたときに両端末で測定したときの加速度を示す．図 4 より両端末で同等の加速度情報を測定することが可能であることがわかる．図 5(a) と図 5(b) に式 (12) によって算出された R'_j と，I_j とをそれぞれ比較した結果を示す．加速度の大きさは異なるものの，バイブレーションが起こった時間が一致することがわかる．

4.2　各端末と予想された波形との比較

加速度の値にはぶれが生じるためそのままの値では一致率が低くなる．3 章で述べたとお

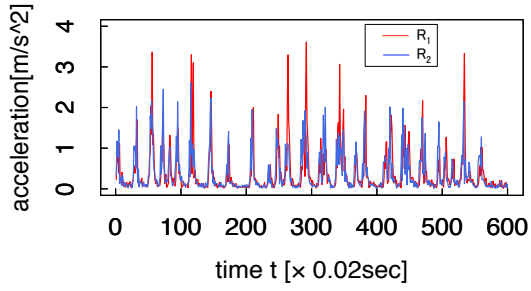
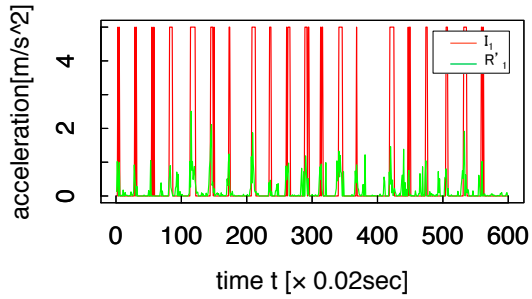
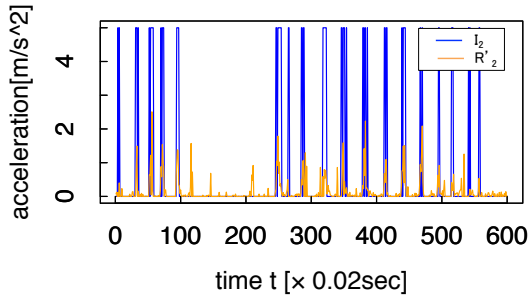


図 4: 各端末で測定した合成波形



(a) d_1 での比較



(b) d_2 での比較

図 5: 予想された加速度と各端末単体で振動させたときに測定した加速度

り，閾値を決め，それをもとに加速度をバイナリデータに変換する．予備実験より，閾値は一致率が最も高くなる各波形の平均値とした．これはこの値のときに一致率が高くなり，妥当だと判断したためである．式 (13) にビット列の一致率 sim を示す．

$$sim = \frac{b_{j,t} \wedge b'_{j,t}}{T} \times 100 \qquad (13)$$

R_1 と R'_1 の一致率は 83.3%，R_2 と R'_2 の一致率は 85.8%となった．

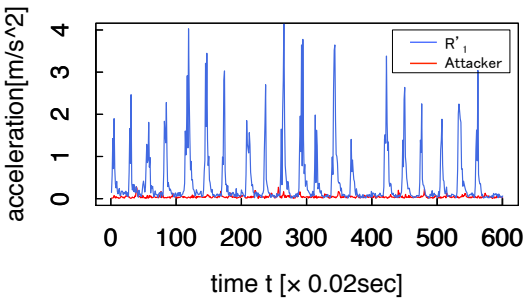


図 6: 攻撃者との比較

4.3 攻撃者との比較

攻撃者は端末 d_1 および端末 d_2 の配置された机上に置くが，端末 d_1 および端末 d_2 とは離れているものとする．図 4 からも分かるように，両端末を振動させたときに各端末で測定された加速度は同じような波形を得られることがわかる．提案方式では端末 d_1 と端末 d_2 を図 2 のように，近接させた状態で評価した．そこで正規の端末と攻撃者との比較を行うために，端末 d_1 と攻撃者の距離を 1 cm 離したときの加速度の測定を行った．図 6 に R'_1 と攻撃者が測定した加速度を示す．R'_1 と攻撃者が測定した加速度の一致率は 53.6%となった．したがって本方式は，攻撃者が正規の端末からわずかに離れた位置に存在している場合においても，安全であることがわかる．

5 おわりに

本研究では秘密を共有したい端末を同一の机上に置き，ある端末にランダムなパターンで振動させ，他の端末は加速度を測定することで各端末が測定した加速度を基に秘密鍵を生成する手法を提案した．提案方式では無線を使用せずに端末間で秘密鍵共有を行うため，中間者攻撃を防ぐことができる．特性評価の結果により，各端末と予想される波形との一致率は R_1 と R'_1 の一致率は 83.3%，R_2 と R'_2 の一致率は 85.8%となった．また攻撃者は 1 cm だけ離れた場合において，R'_1 と攻撃者の一致率は 53.6%となることがわかったため，通信を行う端末の置いてあるテーブルの上に攻撃者がいても，提案方式は守られることが示された．

今後の課題として，提案方式の安全な秘密鍵を生成するのに必要な時間の測定，攻撃者が端末 d_1 と端末 d_2 の間にいたときの対策，バイブレーションを使用した新たな認証方式，攻撃者が b'_j を盗聴していたときの対策，および，３台以上の端末間での利用を想定したプロトコルの提案について検討する．

謝辞

本研究の一部は，「科研費 基盤研究 (C)26420369 高信頼性を有するＩｏＴの実現に向けたセキュアアクセス制御方式に関する研究」の助成により行われた．関係者各位に深謝する．

参考文献

[1] M.Konstantinos et al., “Practical Relay Attack on Contactless Transactions by Using NFC Mobile Phones,” in Radio Frequency Identification System Security, pp.21-32, 2012.

[2] S.Drimer et al., “Keep Your Enemies Close: Distance Bounding Against Smartcard Relay Attacks,” in USENIX Security Symposium, August, 2007.

[3] E.Keogh et al., “Derivative Dynamic Time Warping,” in SDM, pp.2-5, 2001.

[4] T.Halevi et al., “Secure Proximity Detection for NFC Device Based on Ambient Sensor Data,” in ESORICS, pp.379-396, 2012.

[5] T.Halevi et al., “Context-Aware Defences to RFID Unauthorized Reading and Relay Attacks,” IEEE Transactions on Emerging Topics in Computing, vol.1, no.2, pp.307-318, Dec, 2013.

[6] D.Ma et al., “Location-Aware and Safer Cards: Enhancing RFID Security and Privacy via Location Sensing,” IEEE Transactions on Dependable and Secure Computing, vol.10, no.2, pp.57-69, Mar, 2013.

[7] P.Urien et al. “Identity-Based Authentication to Address Relay Attacks in Temperature Sensor-enabled Smartcards,” in European Conference on Smart Objects, Systems and Technologies (SmartSysTech), pp.1-7, Jun, 2013.

[8] M.Miettinen et al., “Context-Based Zero-Interaction Pairing and Key Evolution for Advanced Personal Devices,” in ACM CCS, pp.880-891, 2014.

[9] B.Shrestha et al., “Drone to the Rescue: Relay-Resilient Authentication using Ambient Multi-Sensing,” in International Conference on Financial Cryptography and Data Security, 2014.

[10] Y.Shu et al., “Dynamic Authentication with Sensory Information for the Access Control Systems,” IEEE Transactions on Parallel and Distributed System, vol.25, no.2, pp.427-436, Feb, 2014.

[11] H.Truong et al., “Comparing and Fussing Different Sensor Modalities for Relay Attack Resistance in Zero-Interaction Authentication,” in IEEE PerCom, pp.163-171, 2014.

[12] S.Mathur et al., “ProxiMate: Proximity-Based Secure Pairing Using Ambient Wireless Signals,” in ACM MobiSys, pp.211-224, 2011.

[13] R.Mayrhofer et al., “Shake Well before Use: Intuitive and Secure Pairing of Mobile Devices,” IEEE Transactions on Mobile Computing, vol.8, no.6, pp.792-806, 2009.

[14] T.Wang et al., “Fingerprinting Far Proximity from Radio Emissions,” in ESORICS. Springer, pp.508-525, 2014.