社団法人 情報処理学会 研究報告
IPSJ SIG Technical Report

2009－DPS－138 (52)
2009－CSEC－ 44 (52)
2009／3／6

ユーザの動作類似度に基づく共通鍵生成法

南貴博* 仁野裕一† 野田潤† 中村嘉隆* 関浩之*

モバイル機器の性能向上により，高価もしくはプライバシ性の高いデータが，異なるユーザの端末間でも通信されるようになりつつある．しかし，従来の機器での通信用の暗号鍵は固定的もしくはキー入力による PIN コードを利用したものが一般的で，鍵長は概して短く，鍵の設定は一般ユーザには煩わしい．そこで本稿では，加速度を基にしたユーザ動作対の類似度の高さに従って暗号鍵の生成法を変更し，類似度の高い動作対では短時間に高い強度の共通鍵を，類似度が中程度の動作対ではある程度の時間をかけて共通鍵を生成する手法を提案する．性能評価の結果，類似度は中程度の動作でも，1 分程度で PIN コード相当の共通鍵を生成できることがわかった．

Key Generation from Human Movements for Secure Device Pairing

Takahiro Minami*, Yuichi Nino†, Jun Noda†, Yoshitaka Nakamura* and Hiroyuki Seki*

By the rapid development of the mobile device technology, expensive contents and/or privacy information come to be communicated between the terminals of the users. Currently, as the encrypting key for secure ad-hoc communication, a fixed key or PIN code is commonly used between conventional mobile devices. However, the length of these keys is generally short and the setting of the keys is bothersome. In this paper, we propose a method to generate a common key between mobile devices based on the similarity of the users' movements measured by the accelerometers. The experimental result showed that from a pair of the movements with middle similarity a common key equivalent to the PIN code can be generated within 1 minute.

1 まえがき

モバイル機器の性能向上により，同一人の複数端末間や複数ユーザの端末間でアドホック通信が行うことが可能となってきている．このようなアドホック通信において，商業的価値の高いコンテンツや，プライバシ保護の必要なライフログ等の送受信が，今後益々増大していくと予想される．現状のモバイル機器では暗号鍵として固定もしくはキー入力による PIN コードの利用が一般的となっているが，鍵の設定は一般ユーザには煩わしい．そこで通信の安全性を損なわずに利便性を向上させるような手法として，加速度センサ等の計測情報を一種の端末固有情報として利用することにより，安全に通信し合える端末同士であることの確認や，鍵事前配布のオーバヘッドの減少を目的とした試みがいくつかなされている．[1] では周波数領域上での類似尺度であるコヒーレンス，[2] では量子化高速フーリエ変換 (FFT) を用いて，複数のセンシングデータが同一人の動作によるものかどうかを高い精度で判定する手法を示している．[3] では，2 つのセンサを手にもって振ったときの加速度データに対して，時間領域で主成分分析を行ない，鍵生成を行う手法を提案している．また [4] では，コヒーレンス及び量子化 FFT を利用して鍵生成を行う手法を提案している．

しかし，これらの手法を用いて鍵生成を行うためには，ユーザがセンサを 2 つ合わせて強く振る必要があり，セキュリティ強度の高い鍵を生成できる反面，端末台数が増加した場合や複数のユーザの端末を想定した場合などでは利便性の面で問題がある．高い利便性を達成するためには，通信時の鍵生成について以下 (1)，(2) のような条件を達成できれば望ましい．(1) センサを重ねて強く振るという動作を行わなくても，握手をする，並んでしばらく歩く，自動車に同乗する，といった自然で日常的な動作を行うだけで鍵共有が行えれば，ユーザにとってさらに可用性や親和性が増すと期待される [5]．(2) プライバシ情報の交換からゲームのためのデータ交換まで，求められるセキュリティ強度の面から，種々の応用場面が考えられる．高いセキュリティ強度が求められる場合は非常に類似した動作である場合に限って (長い) 鍵を生成でき，そうでない場合は，鍵長は比較的短くてよいが，ある程度似た動作であれば鍵生成が可能であることが望ましい．

そこで，本研究ではこれらの目標を実現するための，加速度センサに基づく新しい鍵生成法を提案し，その有効性を確認する．

まず，類似度が必ずしも非常に高くはないデータからでも鍵生成が可能となるように，時間領域上の分散値に基づく鍵生成法を新たに提案する．この手法では加速度分散値の時系列データを動的に追跡し，先行する時区間での分散値の平均値をベースラインとして分散値の量子化を行う．これにより「分散値の変化率」に基づき，小さい計算量で，かつ，2 つの動作間の差異を吸収して，多くの場合，同一の値に量子化できる．

また，日常動作から鍵生成を行う場合は，センサを強く振る場合に比べてセンシングデータの変化量が小さいため，類似動作対に対して共通鍵を生成しない確率 (false negative) や，非類似動作対に対して共通鍵を生成する確率 (false positive) が高くなる傾向がある．そこで鍵生成に先立って，2 つの加速度データの時間領域上での分散値の差分，およ

*奈良先端科学技術大学院大学 情報科学研究科
Graduate School of Information Science, Nara Institute of Science and Technology
†日本電気株式会社 サービスプラットフォーム研究所
Service Platform Research Laboratory, NEC Corporation

び，コヒーレンス値を用いて類似度を 2 段階で区分し，鍵生成の可否や鍵生成法を選択することで，false positive を減少させ，かつ鍵長の制御を行う．

量子化 FFT は [4] の手法に基づくが，日常的な動作の場合，仮にコヒーレンス値が高くても，手で振る場合に比べ動作のエネルギーが小さいため 0Hz 付近の重力加速度およびノイズが原因で鍵一致率は非常に低い．そこで，wavelet 変換や量子化幅の調整によって，ノイズの除去を行う．

以上の提案アルゴリズムの有効性を，被験者による実動作データに基づいて評価した．歩行や自動車への乗車など，実際に起こりうるシナリオに基づく動作のセンシングデータ対に基づき鍵生成を行った．その結果，自動車への乗車の場合は 1 分間に約 90bit 相当の，歩行動作では 1 分間で PIN コード相当の鍵が生成できることがわかった．

2 提案手法

2.1 アルゴリズムの概要

鍵生成において安全性の観点から重要なのは，類似しない動作対に対する共通鍵の生成(false positive) をできる限り避けることである．しかし，歩行等の自然な動作の加速度は変化量が小さい．このようなデータに対して，類似度が高いときかつそのときのみ共通鍵(完全に一致したデータ列) を生成するのは困難であるが，一方，類似度だけを定量的に算出することは比較的容易である．そこで提案手法では，加速度の分散値とコヒーレンスという 2 種類の類似度によりデータ対の分類を鍵生成に先立って行うことにより，無駄な周波数領域への変換を省きつつ，false positive を低く抑える．提案する鍵生成手法全体の流れを図 1 に示す．以下に，その概要を説明する．

(1) 加速度の時系列データを区間分割し各区間の分散値を取ることにより，動作の種類をある程度推測できることが予備実験により確認できた．そこで，加速度の時系列データ対に対し，区間ごとにそれらの分散の差分の絶対値を取り閾値と比較する(図 1 の 1 つ目の条件判定．2.2.1 節)．閾値より大きければ鍵生成は行わず，以下であれば，(2) に進む．

(2) コヒーレンスは，周波数領域上の類似尺度であり，0 以上 1 以下の実数値を取り，各周波数の振幅と位相の双方が類似しているほど，1 に近づく．加速度の時系列データを区間分割し各区間を周波数変換する．次にそれらのコヒーレンス値を求めて平均値を取り，閾値と比較し(図 1 の 2 つ目の条件判定．2.2.2 節)，閾値より大きければ量子化 FFT を用いて比較的長い鍵を生成し(2.3.1 節)，そうでなければ分散値を用いて比較的短い鍵を生成する(2.3.2 節)．

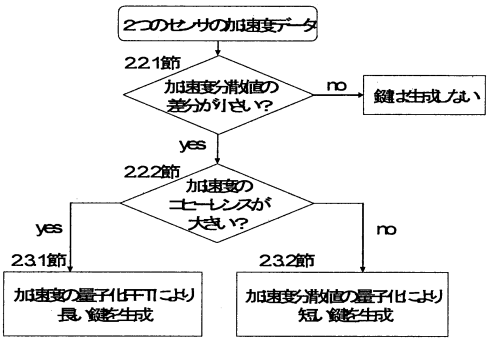

図 1: 鍵生成の流れ

2.2 類似度を利用した動作の分離

2.2.1 分散値による分離

加速度データは，動作によってその揺らぎが異なる．人間の歩行や走行などの揺らぎの大きい動作の場合は，各行動によって加速度の分散値に違いが現れる．そこで 2 つのセンサの加速度分散値を比較し，その差分が小さい場合には類似した動作を，差分が大きい場合は異なる動作をしているとみなして，異なる動作をしている場合を分離する．

2.2.2 コヒーレンスによる分離

分散値の差分では分離できないような似た動作対に対し，コヒーレンスを用いて類似度の判定を行う [1][4]．まず，各センサの取得した波形データを n 分割し，その k 番目のデータをそれぞれ $a_k(t)$, $b_k(t)$ で表す．次に $a_k(t)$, $b_k(t)$ に対して，hann 窓関数 $h(t) = \frac{1-\cos(2\pi t/w)}{2}$ を用いた短時間フーリエ変換 (STFT) を行って，それぞれ各区間 k でのフーリエ係数 $x_k(f) = FFT(a_k(t)\cdot h(t))$, $y_k(f) = FFT(b_k(t)\cdot h(t))$ を得る．この x, y のクロスパワースペクトル $P_{xy}(f)$ は以下のように表すことができる ($\bar{y_k}(f)$ は $y_k(f)$ の共役複素数)．

$$P_{xy}(f) = \frac{1}{n}\sum_{k=0}^{n-1} x_k(f)\bar{y_k}(f) \quad (1)$$

コヒーレンスは以下のように算出される．

$$C_{xy}(f) = \frac{P_{xy}(f)}{P_{xx}(f)P_{yy}(f)} \quad (2)$$

しかし，上記のように波形データ全体に対するコヒーレンス値を算出することは，遅延の増大や追従性の低下を意味する．そこで，データを区間分割し各区間でのコヒーレンスを算出する．本手法では，

図 2 のように，二重窓を用いた区間コヒーレンスを計算する．ここで，W_{out} は区間コヒーレンスを算出する区間を表し，W_{in} は上述のコヒーレンス計算における n 分割した区間 k のサイズを表す．また，外側の窓，内側の窓の双方共に一定量のオーバーラップを設ける．

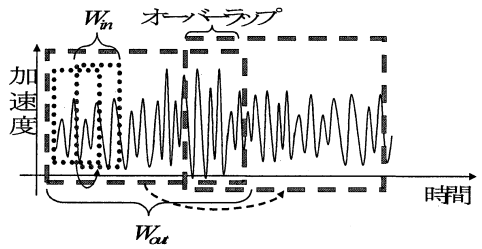

図 2: 区間コヒーレンスの計算

このようにして算出された各周波数帯のコヒーレンス値について，図 3 のように，観測する周波数帯の最大値 (カットオフ周波数と呼ぶ)f^c_{max} を設定し，f^c_{max} までの平均を計算する．

$$C_{xy} = \frac{1}{f^c_{max}} \int_0^{f^c_{max}} C_{xy}(f)dt \qquad (3)$$

この C_{xy} を x，y 間の類似度とする．

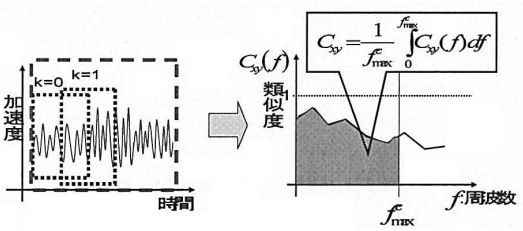

図 3: 類似度の計算

2.3 鍵生成

2.3.1 パワースペクトルからの鍵生成

ここでは [4] で提案されている，以下の量子化 FFT に基づいた方法を改良した鍵生成法を述べる．

(1) 加速度の時系列データをサイズ W_{fft} の小区間 (矩形窓) に分割する．ただし窓は一定の度合でオーバーラップさせる．

(2) 窓内の波形に対して FFT を行い，得られたパワースペクトルのうち周波数 f^q_{max} までを量子化する．低周波が大きく，以降は小さい値に密集するパワースペクトル値の特徴を保存するため，窓内の最大値を基準にし量子バンド幅 (境界線幅) を指数的に増加させる．量子バンド数 (量子化後の値の種類) b は経験的に $b = 5$ 程度がよいとされており，提案法でも予備実験の結果，$b = 5$ を採用した．

(3) 周波数毎の量子値を f^q_{max} まで連結して特徴ベクトルとし，一方向ハッシュ化して互いに交換する．$c \times c$ 通りの特徴ベクトルの組み合わせのうち，一つでも一致するものがあればそれを鍵小片とする．

(4) 鍵小片が得られた窓数の総窓数に対する割合 (一致率とよぶ) が閾値以上であれば，得られた鍵小片を全て連結したものを共通鍵とする．そうでなければ鍵生成は行わない．

センサを重ねて振った場合を鍵生成すべき状況，それ以外を鍵生成すべきでない状況と仮定した場合，上記の手法は優れた性能を発揮する [3]．しかし，日常的な動作の場合，動作量が微小なため性能が劣化してしまう．そこで提案法では量子化について以下の改良を行った．

- 加速度データの低周波には重力加速度等の不要成分が含まれる．そこで Haar wavelet 変換により直流成分と高周波成分を除去し，窓関数 (hann 窓) を作用させてから FFT を行う．
- もはや低周波帯のスペクトルがほとんどないので，量子化値が偏るのを防ぐために，量子化幅は指数的にではなく等間隔に増大させる．

2.3.2 分散値からの鍵生成

分散値は同じ動作が続けば単調な値を示し，歩行 → 停止や，歩行 → 走行など動作が変化した場合は，図 7 のように分散値も激しい変化を示す．提案法はこの特徴に注目し，走行中や歩行中のように同じ動作が連続して分散値の変化が単調になっている部分からは同じ量子値を生成する．また激しく変化した部分からは，その変化に見合った値を生成する．

鍵生成の手順は以下の通りである．なお分散値は，2.1 節の手法で求めたものを使用する．**(1) 分散値の分割**: 分散値の時系列データをサイズ W_{qnt} の小区間 (窓) に分割し一定の度合でオーバーラップさせる．また，量子化に必要な境界線のベースラインを決定するために W_{qnt} より過去の分散値を，サイズ W_{pre} だけ抜き出す．**(2) 境界線の設定**: W_{pre} の平均値を基準に，図 4 のように等間隔の境界線を引き，b 個の量子バンドを設ける．そして W_{qnt} での平均値が含まれている境界に割り振られた値で量子化する．また量子バンド幅に変化を持たせて，候補を複数生成する．**(3) 特徴ベクトルの生成**：求めた 2 センサの量子値を 1 桁ごとに比較した場合，W_{qnt} での平均値に大きな差があったとしても，候補値のどれか 1 つが偶然一致してしまうことがある (false positive)．このようにして求めた量子値を順に L 個連結させた後に比較することで false positive の割合を低く抑えた．ただし連結するときは，同一の境

界幅で求めた量子値同士を連結させる (よって連結後も候補数は c 個である). この連結した L 個の量子値を特徴ベクトルとする. **(4) 特徴ベクトルの比較**: 2.3.1 節の (3), (4) と同様に, 一致した特徴ベクトルを連結して共通鍵とする.

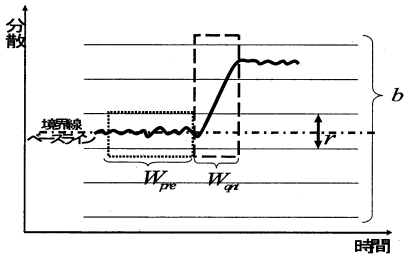

図 4: 分散値量子化

3 評価実験

3.1 実験環境

本実験では, 動作の加速度計測に 表 1 の 3 軸加速度センサ (Wireless-T 社製 WAA-001) を使用した. 加速度センサのサンプリング率は 50Hz に設定して各実験の計測を行った. センサは各被験者の胸と腰の 2 ヶ所に装着し, データ収集用のノート PC を 1 台持たせ, センサのデータを Bluetooth を用いて PC に送信する.

表 1: 加速度センサの仕様

サイズ	38 × 39 × 10mm
重量	17g
検出軸数	3 軸
検出範囲	±3G
最大サンプリング率	200Hz

3.2 実験動作とシナリオ

歩行実験 3 人の被験者が 30 分程度, 同じルートを移動したときの加速度を計測した. 街中を移動している状況を再現するため, 計測中は歩行だけではなく, 走行や停止といった動作も行った. また被験者には以下のような役割を与えた.

- **先導**: ルートを好きなペースで移動する.
- **並行**: 先導役に並び歩調を合わせて移動する.
- **自由**: 誰の歩調も意識せず先導役の周辺 (20〜30 メートル) を自由に動き回る.

このときに計測した加速度データを図 5 に示す.

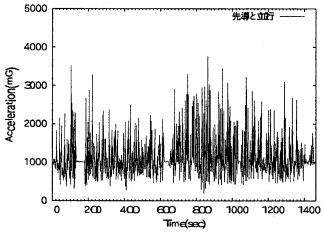

図 5: 加速度:歩行

乗車実験 3 人の被験者が 2 台の自動車に分乗し, 10 分程度のルートを移動したときの加速度を測定した. 被験者 3 人には以下のような役割を与えた.

- **先導**: ルートを先導する車に乗る.
- **同乗**: 先導役と同じ車に乗る.
- **追走**: 先導役が乗る車を追走する車に乗る.

このときに計測した加速度データを図 6 に示す.

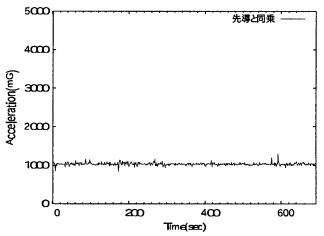

図 6: 加速度:乗車

3.3 評価結果

3.3.1 分離について

実験では胸と腰の加速度データに特に大きな差は見られなかった. そこで本稿では, 主に腰のセンサから得られた加速度データを用いて提案法の検証を行う. また各実験データは完全に時間同期されていると仮定する. 分散値の差分による分離を行うために, 分散値を求める窓サイズを $W_{var} = 150$, 窓のオーバーラップを 50% に固定し, 分散値の差分の平均を求めた. 各動作の分散値とその差分の例を図 7 および図 8 に示す. このときの差分の平均値は表 2 のような結果となった.

表 2: 分散値の差分平均値

歩行実験		乗車実験	
並行	自由	同乗	追走
0.325	1.187	0.231	0.707

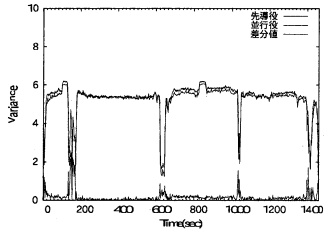

図 7: 分散値と 差分:歩行

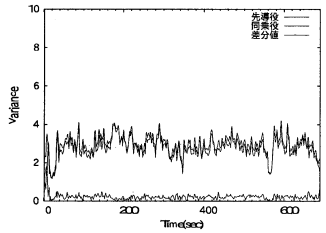

図 8: 分散値と 差分:乗車

また，コヒーレンスによる分離を行うために内窓と外窓のサイズを $W_{in} = 64$, $W_{out} = 512$，窓のオーバーラップを 50% に設定し，比較する周波数帯の上限値 f^c_{max} を変化させてコヒーレンスの値を求めた．各動作のコヒーレンス平均値は 表 3 のような結果となった．また，歩行実験の先導と 並行のコヒーレンス値の時系列変化を図 9，乗車実験の先導と 同乗の場合の時系列変化を図 10 に示す．

表 3: コヒーレンスの平均値

	歩行実験		乗車実験	
	並行	自由	同乗	追走
f^c_{max}=5Hz	0.135	0.109	0.647	0.081
f^c_{max}=10Hz	0.107	0.091	0.670	0.076
f^c_{max}=15Hz	0.098	0.083	0.615	0.072
f^c_{max}=25Hz	0.096	0.080	0.538	0.071

3.3.2 鍵生成について

パワースペクトルを用いる手法の各パラメータを表 4 のように設定し，パワースペクトルからの鍵生成を行った．分離によってこの鍵生成法が適用される主な動作は乗車であることを考慮し，乗車における先導役と 同乗役および先導役と 追走役の 2 種類の組み合わせから鍵生成を行った．その結果生成された鍵の一致率と 1 分あたりに生成される 平均鍵長は表 5 のようになった．1 桁あたりの量子値は 5 種類だが以降鍵長は 2 進数に換算して記述する．

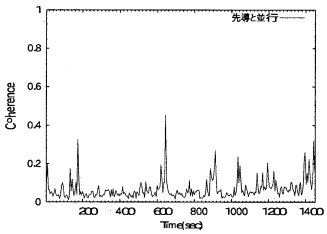

図 9: コヒーレンス:歩行

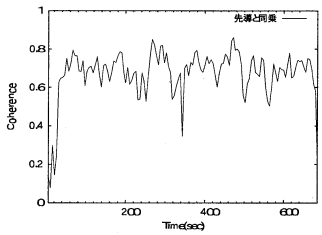

図 10: コヒーレンス:乗車

表 4: パワースペクトル量子化のパラメータ

パラメータ	値
W_{fft} (FFT の窓サイズ)	64, 128
W_{fft} のオーバーラップ	50%
b (量子バンド数)	5
c (量子値の候補数)	6
α (境界の増加幅)	0.333
f^q_{max} (量子化する周波数帯最大値)	10Hz

表 5: パワースペクトルからの鍵生成

乗車 同乗 分散差分:小 & コヒーレンス:大			
$W_{fft} = 64$		128	
一致率	鍵長	一致率	鍵長
16.0%	179.8 桁 417.6 bit	7.2%	84.5 桁 196.2 bit

また，分散値を用いる手法の各パラメータを表6のように設定し，鍵生成を行った．分離によってこの鍵生成法が適用される主な動作は歩行であることを考慮し，歩行における先導役と並行役および先導役と自由役の2種類の組み合わせから鍵生成を行った．その結果生成された鍵の一致率と1分あたりに生成される平均鍵長は表7のようになった．

表 6: 分散値量子化のパラメータ

パラメータ	値
W_{var} (分散算出の窓サイズ)	150
W_{qnt} (量子化対象の窓サイズ)	5, 10, 20
W_{pre} (過去データ窓サイズ)	$W_{qnt} \times 3$
W_{var}, W_{qnt} のオーバーラップ	50%
r (境界幅の初期値)	0.3, 0.5, 0.7
b (量子バンド数)	5
c (量子値の候補数)	4
α(境界の増加幅)	0.166
L (量子値の連結数)	3

表 7: 分散値からの鍵生成

	歩行 先導と並行 分散差分:小 & コヒーレンス:小					
	W_{qnt}=5		10		20	
	一致率	鍵長	一致率	鍵長	一致率	鍵長
r=0.3	97.1%	29.1bit	98.4%	17.1bit	96.6%	7.9bit
r=0.5	98.1%	29.4bit	98.4%	17.1bit	96.6%	7.9bit
r=0.7	98.1%	29.4bit	98.4%	17.1bit	100%	8.2bit

3.4 考察

1. 分散による分離に関する考察: 表2から，歩行，乗車いずれの場合も類似の動作とそれ以外をよく分離できていることが分かる．追走の場合，鍵共有を拒否するかどうかは状況や応用に依存する．拒否としたい場合は閾値を低く設定すればよい．また，静止している箇所の分散値差分が大きくなってしまっている．これは分散の対数値で差分を求めているため，分散値の低い個所は小さな揺らぎも大きな差として判断してしまうのが原因である．

2. コヒーレンスによる分離に関する考察: 表3の通り，歩行実験ではいずれの対もコヒーレンス値は小さく，乗車実験では同乗と追走をよく分離している．また一人の被験者が装着した胸と腰のセンサ間のコヒーレンス値も平均0.3程度の低い値となることから，一見よく似ているデータ対でも，位相の違いによって確実に分離できることが分かった．

3. パワースペクトルからの鍵生成に関する考察: 表5の通り，一致率は低いが比較的長い鍵を生成することに成功した．パラメータを表6の通りに設定したとき，1つの特徴ベクトルは約28bit相当である．そのうち一致，不一致に関わらず全乗車データから生成された特徴ベクトルは，50707種類(約15bit)となった．また，10分の乗車データ(先導と同乗)から生成された全特徴ベクトルは5395種類(約12bit)で，そのうち一致した特徴ベクトルは85個(約6bit)となった．従って表5の $W_{fft} = 64$ のとき，$417 * 6/28 = 89.35$ bit となり1分間で約90bit相当の鍵ができることになる．

4. 分散値からの鍵生成に関する考察: 分散値からの鍵生成は表7の通り，歩行の動作からは一致率の非常に高い鍵を生成することに成功した．実験データでは，$W_{qnt} = 5$ が鍵長，一致率共に良い結果となった．しかし W_{qnt} を小さくとりすぎると，動作のずれから受ける影響が大きくなることに注意が必要である．パラメータを表6と $W_{qnt} = 5$，$r = 0.5$ に設定したとき，1つの特徴ベクトルは約7bit相当である．このとき全歩行データから生成される特徴ベクトルは72種類(6bit)であった．また，30分の歩行データ(先導と並行)から生成された全特徴ベクトルは26種類(4〜5bit)で，そのうち一致して鍵の要素となった特徴ベクトルは16個(4bit)となった．よって動作変化に富む箇所からは，1分程度で $29 * 4/7 = 16$ bit と PINコード相当(13bit)の鍵生成が可能である．

4 あとがき

本研究では歩行や自動車への乗車など日常的な動作を利用して鍵生成を行うために，各動作の類似度を加速度の分散値やコヒーレンスを利用して判定し，類似度に応じて強度の異なる鍵を生成する手法の提案を行った．性能評価の結果，振動パタンが異なる日常的な歩行や乗車といった動作から提案手法に基づき鍵生成が可能なことを確認した．

参考文献

[1] J. Lester, B. Hannaford, and G. Borriello. "Are You With Me?" - Using accelerometers to determine if two devices are carried by the same person. Pervasive2004, LNCS 3001, pp.33-50, 2004.

[2] Y. Huynh and B. Schiele. Analyzing features for activity recognition. sOc-EUSAI'05, pp.159-163, 2005.

[3] D. Bichler, G. Stromberg, M. Huemer, and M. Low. Key generation based on acceleration data of shaking processes. UbiComp2007, LNCS 4717, pp.304-417, 2007.

[4] R. Mayrhofer and H. Gellersen. Shake well before use: Authentication based on accelerometer data. Pervasive2007, LNCS 4480, pp.144-161, 2007.

[5] 仁野裕一, 野田潤, 中尾敏康. 携帯電話の操作履歴情報を利用した認証方式の提案. DICOMO2007.