Secret Key Agreement Scheme Based on Phase Variation of Fading in Mobile Communications

Hiroki NAKAI*, Hideichi SASAOKA* and Hisato IWAI*

(Received April 20, 2018)

Recently, a secret key agreement scheme using radio propagation characteristics has been studied as a countermeasure against eavesdropping in wireless communication. Most of secret key agreement schemes using radio propagation characteristics uses quantization of sample value of the received signal strength variation. This paper proposes a method of sharing secret key using level crossing time information based on a phase difference variation that is not considered. In the proposed system, each station alternately transmits and receives signal and measures the propagation characteristics. In order to reduce the influence of noise, the noise is removed from received signal by using filter in frequency domain. From the measured radio propagation characteristics at the transmitter station, set a certain sample value to the standard value. The standard value to detect a level crossing is transmitted from a transmitter station to a receiving station through a public channel. The receiving station acquires time information when a level cross for the standard value. The information of the level crossing time is acquired continually by repetition of this processing. After the receiving station calculates existing space data between the acquired time, the space data is encoded to binary. The binary encoding bit is a bit sequence for secret key generation.

Key words : radio propagation characteristics, secret key agreement scheme, phase difference, level crossing time information

キーワード：電波伝搬特性，秘密鍵共有方式，位相差，レベル交差時刻情報

移動通信におけるフェージングの位相変動に基づく秘密鍵共有方式の研究

中井　宏樹，笹岡　秀一，岩井　誠人

1. はじめに

近年，無線通信の利便性の高さから携帯電話やスマートフォンなどが急速に普及している．無線通信では，電波が空間中を伝搬して情報を送受信するため，第三者による盗聴や不正アクセスなどが容易となり，情報セキュリティ上で脆弱性の問題が発生する．そのため安全な通信を実現するための盗聴対策が重要となる．その盗聴対策として暗号化によるセキュリティ技術が提案されており，一般に計算量的な複雑性に基づいた安全性を持つ公開鍵暗号方式や共通鍵暗号方式がある．移動通信の場合，公開鍵暗号方式では処理演算能力に制約があることから，一般的に共通鍵暗号方式が用いられる．この共通鍵暗号方式は暗号化と復号に同一の鍵を使用するため，

*Department of Electronics, Doshisha University, Kyoto
Telephone: +81-774-65-6355, FAX: +81-774-65-6801, E-mail: hsasaoka@mail.doshisha.ac.jp

鍵配送や鍵管理の安全性が課題となる[1].

そこで鍵配送・鍵管理の必要性がない情報量的な複雑性を根拠とする物理層セキュリティ技術として，電波伝搬特性を活用した秘密鍵共有方式[2]が研究されている．この電波伝搬特性とは，基地局と移動局との間で同じ時間に同じ周波数で信号を送受信すれば両局で同じフェージング変動を受信するという電波伝搬の可逆性と観測点から半波長程度離れると相関係数は急速に減少するという場所依存性という 2 つの特性を示す．これにより，盗聴局に知られることなく，安全な秘密鍵を共有することができる．

従来の秘密鍵共有方式には，受信信号強度変動に基づき設定した閾値に対して標本値の大小を判定し，量子化することで鍵生成を行うものが大半である[3]. しかし，送受信機の増幅器の増幅率の違いにより，絶対値を用いることは困難となるため，中央値や平均値を閾値とするなどの対策が必要となる．これは位相の場合でも，局部発振器の周波数差による位相ずれにより絶対位相を用いることは困難となるため，相対位相とするなどの対策が必要である[4].

また，フェージング変動が低速な屋内環境などで鍵長の長い鍵を時間内に作成するには，伝搬路変動が高速，且つ，電波伝搬特性の観測が高精度に行う必要がある．このような場合には，時刻情報を活用した秘密鍵共有法が有効となる可能性がある[5].

そこで本論文では，電波伝搬特性の変動が比較的緩やかな環境を想定し，相対位相の時間変動に基づいた時刻情報を活用した秘密鍵共有方式を提案する．相対位相とすることで送受信機の局部発振器の周波数差を除去することが可能となる．

2. 電波伝搬特性を用いた秘密鍵共有方式

2.1 電波伝搬特性に基づく秘密鍵共有方式

電波伝搬特性に基づく秘密鍵共有方式は電波伝搬の可逆性と場所依存性に基づいている．そのため，盗聴局が異なる場所で正規局間の電波伝搬特性を推定することはほぼ不可能となり，正規局間で観測した伝搬特性から鍵を生成することで秘密裏に鍵の共有が行える．従来の秘密鍵共有方式では受信信号強度を用いた方式が大半である[3]. その概念図を Fig. 1 に示す．この方式ではまず，正規局それぞれで受信信号強度を観測する．その後，観測結果を元に閾値（中央値や平均値）を設定し，標本値の大小判定を行い，量子化することで秘密鍵の生成を行う．これが電波伝搬特性を用いた最も簡易的な秘密鍵共有法である．また，秘密鍵生成の速度はフェージング変動の速さに依存する．伝搬路変動が比較的緩やかな屋内環境などでは，伝搬特性の時間変動が小さくなるため，標本値を量子化して鍵生成を行うには標本間隔を広く設定する必要がある．そのため，十分な鍵長を持つ秘密鍵を生成するには長時間の観測が必要となる．このような場合には複数アンテナの重みを制御して伝搬特性を観測することで人為的なフェージング変動を発生できるため，鍵生成の速度を早めることができる[6].

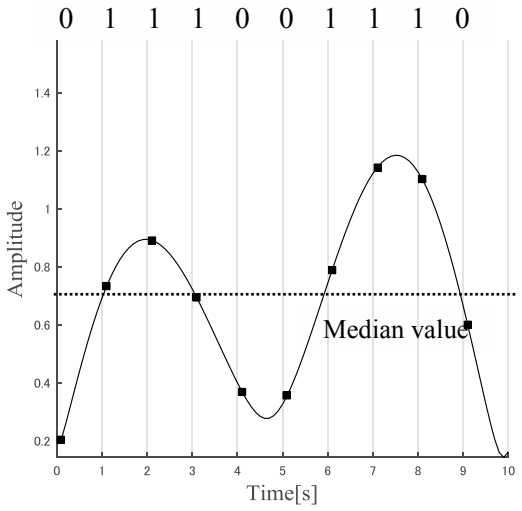


Fig. 1. Binary code generation method by median value.

2.2 相互情報量・秘密鍵容量

電波伝搬特性を用いた秘密鍵共有方式は相関情報を用いた秘密鍵共有方式に分類される．ここで，秘密鍵共有プロトコルは，① Advantage distillation，② Information reconciliation，③ Privacy amplification の三段階で構成される．段階①では，正規局間で共有する相互情報量が盗聴局と共有する相互情報量よりも大きくなる乱数を生成する．段階②では公開通信路を通して正規局間で情報交換し，乱数系列を一致させる．段階③では正規局間で一致している乱数系

列から盗聴局が知ることのできない秘密鍵を生成し，鍵共有を行う．これらの段階を理想的に行った場合に盗聴局に知られないで正規局間のみで共有することができる情報量として秘密鍵容量が検討されており，これは秘密鍵の期待値を示す．ここで確率変数 X，Y，Z が多値である場合，その各 2 進符号化ビットは $X=(X_1, X_2, \ldots, X_k)$ と表現され，各 2 進符号化ビットのエントロピー関数 H は次のようになる．

$$H(X_k) = -P_{X_k}\log_2 P_{X_k} - (1-P_{X_k})\log_2(1-P_{X_k}) \quad (1)$$

また，結合エントロピー $H(X_k, Y_k)$，$H(X_k, Y_k, Z_k)$ は

$$H(X_k, Y_k) = -P_{X_kY_k}\log_2 P_{X_kY_k} - \left(1-P_{X_kY_k}\right)\log_2(1-P_{X_kY_k}) \quad (2)$$

と表される．ここで，$P_{X_kY_k}$ は X-Y 局間における各 2 進符号化ビットの不一致率を示す．この不一致率導出については 3.4 節で記載する．以上，式（1）と式（2）より以下の条件つきエントロピーを算出する．

$$H(X_k|Y_k)=H(X_k,Y_k)-H(Y_k) \quad (3)$$

以上より，相互情報量 $I(X_k;Y_k)$，秘密鍵容量 $S(X_k;Y_k||Z_k)$ の下限は以下の式で表現される [7]．

$$I(X_k;Y_k) = H(X_k) - H(X_k|Y_k) = H(Y_k) - H(Y_k|X_k) \quad (4)$$

$$S(X_k;Y_k||Z_k) \geq \max[I(X_k;Y_k) - I(X_k;Z_k), I(X_k;Y_k) - I(Y_k;Z_k)] \quad (5)$$

3. レベル交差時刻情報に基づく秘密鍵共有法

3.1 時刻情報を用いる利点

電波伝搬特性に基づく秘密鍵共有方式の大半は標本値を量子化して鍵生成を行うものである．この方法において，限られた時間内に十分な鍵長の秘密鍵を生成し共有するには，フェージング変動が高速であること，また，電波伝搬特性の測定を高精度に行う必要がある．電波伝搬特性の変動が緩やかな環境の場合では，標本間隔をフェージングの変動周期に応じて長く設定する必要がある．仮に，標本間隔を短く設定すると，見かけ上鍵長の長い秘密鍵を生成可能となるが，標本値間の相関が高くなるため鍵ビットは無相関でなくなり，取得した鍵の秘密鍵容量は標本点数の増加に応じて増加しない．そのため高速の鍵生成は困難となる．Fig. 2 には標本間隔を狭く設定した場合の鍵ビット作成の様子を示している．

一方で，電波伝搬特性があるレベル（閾値）を交差する時刻情報を元に秘密鍵の生成を行う場合，その情報量は標本間隔に依存し，ビットの生成量に比例する．このため伝搬特性の測定精度に依存して，標本間隔を細かく設定できる．これが時刻情報を用いる利点である．標本間隔を狭く設定しながらレベル交差する時刻情報を共有して秘密鍵の生成を行うには，受信機による雑音の抑制やレベル交差時刻の不一致低減などの対策が必要となる．

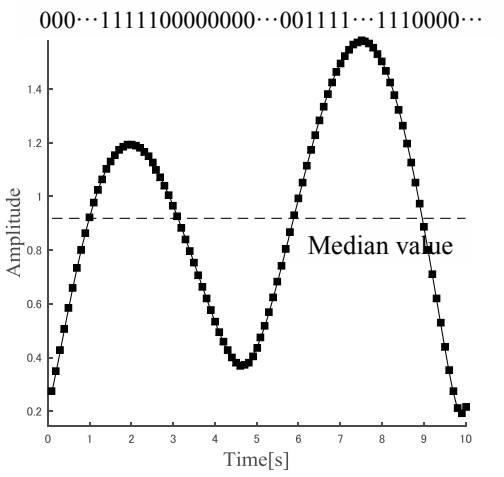


Fig. 2. Binary code generation method by median value (The sampling interval is narrow).

3.2 位相差の時間変動導出

従来方式において，正規局間で同一の伝搬特性を測定することは可能であるが，増幅器の増幅率の違いにより信号強度値に誤差が発生する．そのため閾値に絶対値を用いることは困難となるため，各局において中央値や平均値を閾値とするなどの工夫が必要となる．仮にフェージングの位相変動に基づいて閾値を設定した場合でも，局部発振器の周波数差により誤差が発生するため，相対位相を用いるなどの工夫が必要となる．そこで本論文では複数の周波数の異なる信号を伝送し，その中の 2 波の掛け合わせにより導出する．位相差をとることで両局間の局部発振器の周波数差を除去できるため，閾値に位相差の時間変動の絶対位相を用いることが容易となる．この導出方法について Fig. 3 に基づいて説明する．

想定する伝搬路は伝送帯域幅が広帯域でフェージング変動が一様ではなく，周波数ごとに変動の様子が異なる周波数選択性フェージングとし，周波数の異なる 2 波のフェージングによる位相変動の差を位相差の時間変動として用いる．まず，送信局で広帯域幅内から周波数の異なる 2 波S_1, S_2を選択する．その後，局部発振器により搬送波周波数をf_cとした搬送波変調を受ける．f_1, f_2は各波の周波数，θ_1, θ_2は初期位相を示す．送信信号は伝搬路（伝搬路変動は$|H(f_1)|e^{j\varphi_1}$，$|H(f_2)|e^{j\varphi_2}$と表している）を通り受信局へ到達する．到達した 2 波の合成波（受信波）は復調された後，各々の波r_1, r_2に変換される．ここで，受信波r_1, r_2は以下のように表される．

$$r_1 = |H(f_1)|e^{j(2\pi(f_1+\Delta f)t+\theta_1+\varphi_1)} \quad (6)$$

$$r_2 = |H(f_2)|e^{j(2\pi(f_2+\Delta f)t+\theta_2+\varphi_2)} \quad (7)$$

Δfは送信局側と受信局側における局部発振器の周波数差である．その後，受信波r_2の複素共役をとり，その 2 波を掛けあわせ，周波数成分と初期位相成分を除去することでフェージングによる位相変動の差 $e^{j(\varphi_1-\varphi_2)}$ を算出する．最終的な受信信号rは以下のようになる．

$$r = |H(f_1)||H(f_2)|e^{j(\varphi_1-\varphi_2)} \quad (8)$$

以上の過程により，位相差の時間変動を算出する．

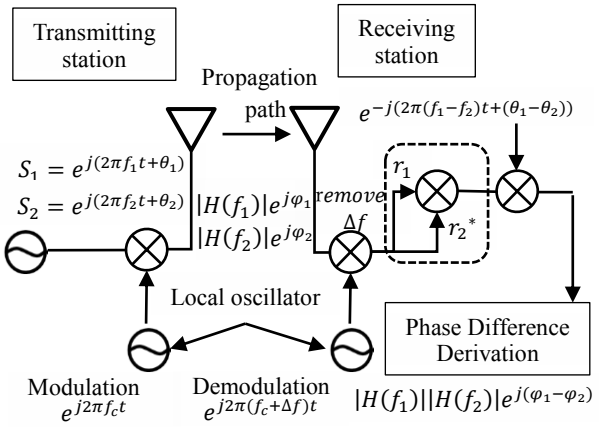


Fig. 3. Time change derivation process of the phase difference.

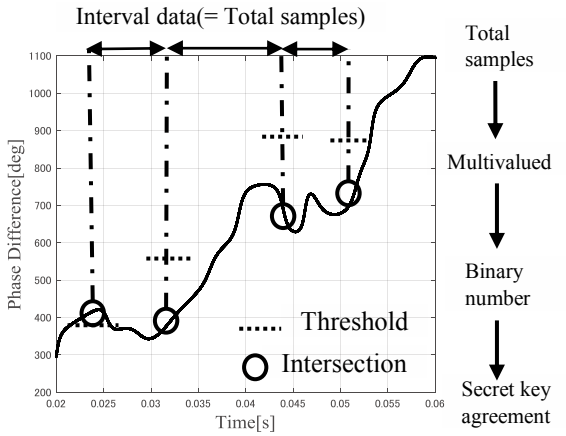


Fig. 4. Principle of the secret key agreement using the level crossing time.

3.3 レベル交差時刻情報を用いた秘密鍵共有の原理

Fig. 4 に位相差の時間変動に基づいた時刻情報を活用した秘密鍵生成の流れの例を示す．フェージングの位相変動や信号強度変動が閾値などの基準値(レベル)を交差する時刻情報を共有する場合，その情報量は標本間隔の細かさに依存する．そこで標本値間の標本間隔は細かく設定している．まず，観測した電波伝搬特性に基づいてある基準値を設定する．設定後，電波伝搬特性の時間変動がレベルとなる基準値を交差する時刻情報を取得する．この処理を繰り返して，レベル交差時刻間の間隔データを算出し，それを用いて秘密鍵生成を行う．ここで，正規局間における時刻情報に誤差が発生すると間隔データも相違する．これは受信機雑音の影響によるものであるが，この低減方法については次節で説明することにする．具体的に鍵の元となる鍵ビットはそのレベル交差時刻間に存在する標本の総数を多値量子化し，2 進符号化する．このため標本数が多いほど鍵ビットの生成量は多くなる．また，本論文のような位相差の時間変動に基づく場合，基準値を固定値とするとレベル交差が頻繁に出現せず，限られた時間内で秘密鍵を生成することは困難となる．そのため本方式では，固定値ではなく伝搬特性の観測結果に対して臨機応変に基準値を設定する．本方式における基準値の設定方法に関する詳しい説明は 3.5 節で記載する．

3.4 レベル交差時刻検出の精度向上対策

3.4.1 レベル交差時刻検出の誤差の要因

受信機雑音による正規局間での時刻情報の不一致

を軽減させるために周波数領域においてフィルタによる信号成分の切り出しを行う [8]．フィルタの大きさは最大ドップラー周波数の 4 倍程度とし，雑音低減後の伝搬特性が低減前の伝搬特性と比較して歪まない程度の大きさとした．ここで，フィルタ処理により雑音の低減を行っても，完全な雑音除去は困難なため，設定する基準値によっては，正規局間でもレベル交差時刻が大幅にずれる場合がある．そのため，設定する基準値の領域を見定める必要がある．Fig. 5 に正規局間におけるレベル交差時刻検出の誤差の例を示す．範囲 A のような傾きが急峻な伝搬特性の観測部分から基準値を設定した場合，両局間との時刻検出誤差は小さくなる．しかし，範囲 B と C のような傾きの緩やかな観測部分では時刻検出誤差が顕著となって現れている．以上のことから，山や谷周辺の傾きの緩やかな領域からではなく，ある程度の傾きを持った急峻な領域から基準値を設定する必要がある．

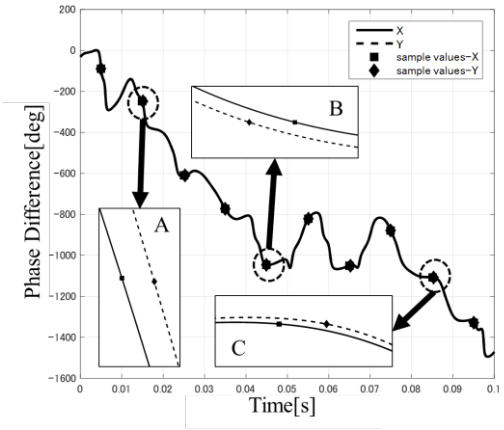


Fig. 5. Factor of the detection time error.

3.4.2 適切な基準値を設定する時間領域の選択法

次に傾きの緩やかな領域から基準値を設定しないために 2 つの条件を課すことにする．

条件 1：隣接標本値間の位相変動幅が下限以上，上限以下

本研究では標本間隔を非常に細かく設定しているため，標本値間の位相変動幅は非常に小さくなる．特に傾きの緩やかな領域では標本値間の値はほぼ同一となるため正規局間で大幅に検出時刻がずれてしまう．そこで基準値の設定可能領域を隣接標本値間の位相変動幅に対して下限と上限を設定し，領域を限定することにより，標本値検出時刻（レベル交差時刻検出）誤差の低減をはかる．具体的には Fig. 6 より，標本値 A と標本値 B の位相変動幅が設定した下限以下もしくは上限以上であれば，基準値の設定可能領域とはせず，下限以上，上限以下であれば基準値の設定可能領域として用いる．

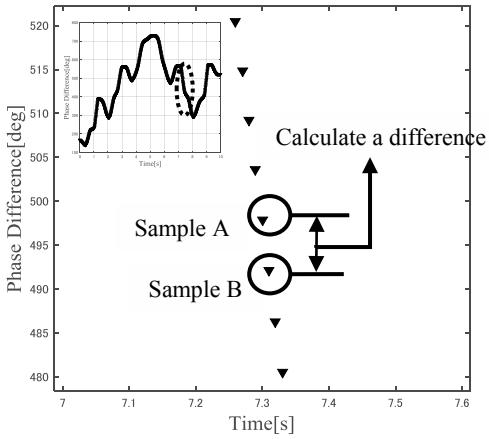
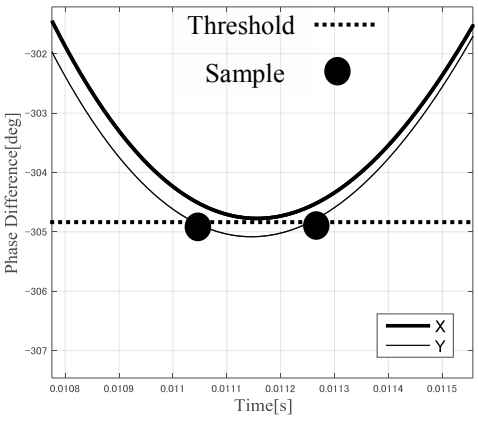


Fig. 6. Angle difference derivation method between sample values.

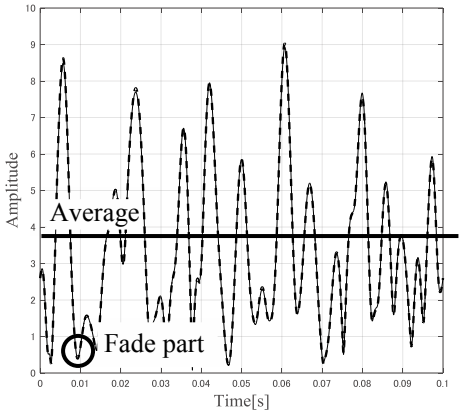
条件 2：受信信号強度の低下領域の回避

雑音の影響により極大値や極小値周辺から基準値を設定すると標本値の検出時刻誤差が発生する可能性が高くなる．また，場合によってはレベル交差が一方の正規局しか起こらない時もある．これは受信信号強度の減衰領域と深く関係している．

Fig. 7 に受信信号強度の減衰領域(b)に対する位相差の時間変動の様子(a)を示す．(a)より X 局では位相差の時間変動と基準値が交差しているのに対して，Y 局では交差していない．そこで誤差発生の要因となる信号強度の減衰領域からの基準値の設定を回避するために，信号強度値の平均値の 2 分の 1 以下から基準値の設定は行わないものとする．ここで条件 1 も踏まえ，平均値以下と設定すれば，基準値設定可能領域は非常に狭くなるため，基準値設定回数の頻度の低下により限られた時間内での秘密鍵生成が困難となる．



(a) Detect or undetect of intersection.



(b) Fade of the amplitude.

Fig. 7. Deletion of the amplitude fade part.

3.5 提案方式の構成

以上の内容を踏まえ，Fig. 8 に本論文おける提案方式の構成を示す．まず，公開通信路を通して正規局間で送受を切り替えて同一の電波伝搬特性を観測する．マルチパス伝搬路において受信信号は不規則に変動するため，場所依存性により正規局間のみで同一の伝搬特性を得ることができる．次に，観測した伝搬特性の傾きの急峻な観測領域から送信局（X 局）である標本値をランダムに基準値として設定する．その後，その基準値は受信局（Y 局）へ送信される．Y 局ではその設定した基準値を交差する標本値の検出時刻を取得する．

この模式図を Fig. 9 に示す．ここで，フェージング周期（最大ドップラー周波数の逆数）を 1 ブロックとし，正規局間におけるその同ブロック内において一方の局では標本値検出時刻を取得しない場合がある．そこで Y 局において X 局と同一のブロック内で標本値を検出または未検出の判断を下し，その処理結果について X 局へ通達する．もし Y 局が標本値検出時刻を取得すれば X 局でも標本値検出時刻の取得を行い，Y 局で取得しなければ X 局も取得しない．このような処理により，電波伝搬特性の観測に基づきながら時刻情報の取得を行う．そして時刻情報間に存在する間隔データを多値量子化し，2 進符号化することで鍵生成のためのビット系列を作成し，秘密鍵として共有する．

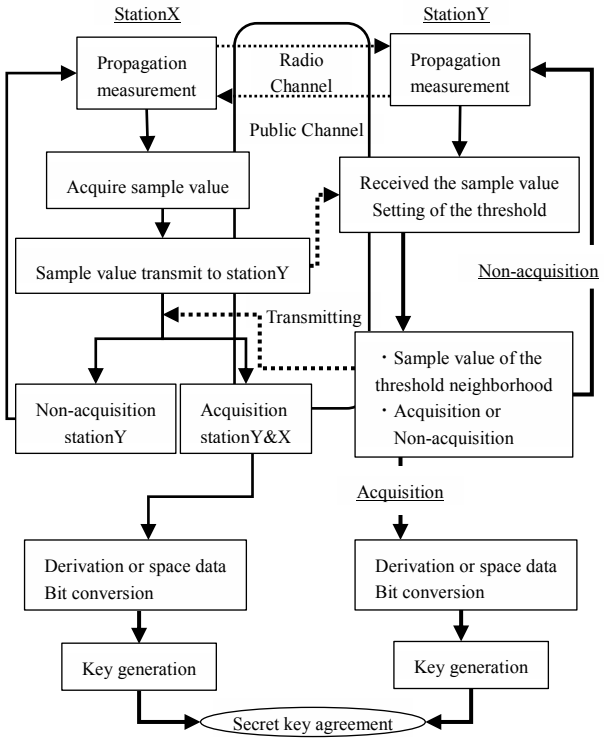


Fig. 8. Configuration of proposed system.

3.6 各 2 進符号化ビットの特性評価方法

提案方式では位相差の時間変動に基づいてレベル交差時刻情報から間隔データを算出し，2 進符号化することにより秘密鍵の生成を行う．ここで，符号化後の評価対象とするビット長は正規局においてその出現確率が 100%のビットとそこに余裕を持たせて 1 ビット追加したビット長とする．結果として 100%出現したのは第 14 ビットまででであったため，

第 15 ビットまでを評価の対象とし, 盗聴局側における特性の評価においても第 15 ビットまでの評価とする．また, 例えば正規局間では第 15 ビットまで出現し，盗聴局側では第 14 ビットまで出現した場合，盗聴局側の第 15 ビットに「0」を加え，桁合せを行ってから評価する．作成された 2 進符号化ビットは雑音の影響によりレベル交差時刻に誤差が発生すると，正規局間でもその交差時刻間に存在する間隔データに差異が生じるため，相違してしまう．そのため多少の誤差であってもビット系列内の下位ビットではビット誤りの発生が考えられる．したがって，鍵生成に最適なビットを定めるため，各 2 進符号化ビットの特性について調査する．その特性を表す指標の一つに 2.2 節に示す秘密鍵容量があるが，この導出には各 2 進符号化ビットの不一致率が必要となる．

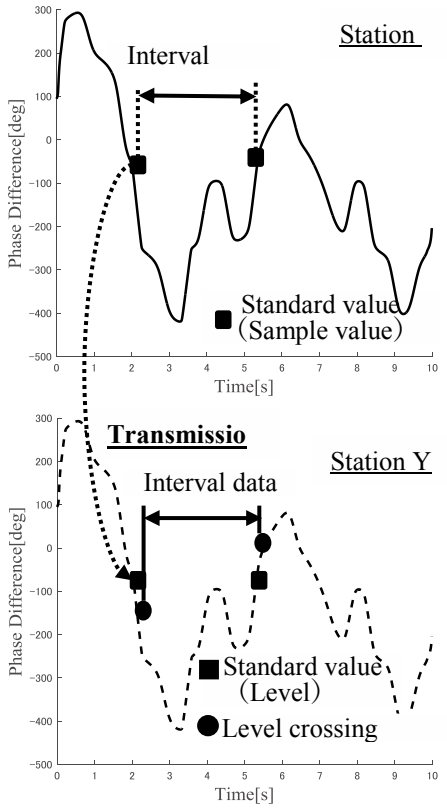


Fig. 9. The sample value detection after the standard value intersection.

そこで Fig. 10 を例にその不一致率の導出方法について説明する．まず，ある時刻間の間隔データを 2 進符号化したビット系列を X 局では「101…0101」，Y 局では「101…0111」とする．2 つのビット系列の差を求めると「000…0010」となり，不一致系列 E の算出が可能となる．不一致系列内において「0」は両局間で一致しているビットであり，「1」は不一致であるビットを示す．この処理を繰り返し，複数の不一致系列を算出した後，式 (9) を用いて不一致率 $P_{X_kY_k}$ を導出する．

ここで，E は不一致系列であり，k はその不一致系列の個数を表す．また, i はビット系列における各 2 進符号化ビットのビット番号である．このビット番号は下位ビット側から順番に第 1 ビット，第 2 ビット・・・第 n ビットと称する．

$$P_{X_kY_k} = \frac{\sum_{j=1}^{k}(E_{ji}=1)}{k} \tag{9}$$

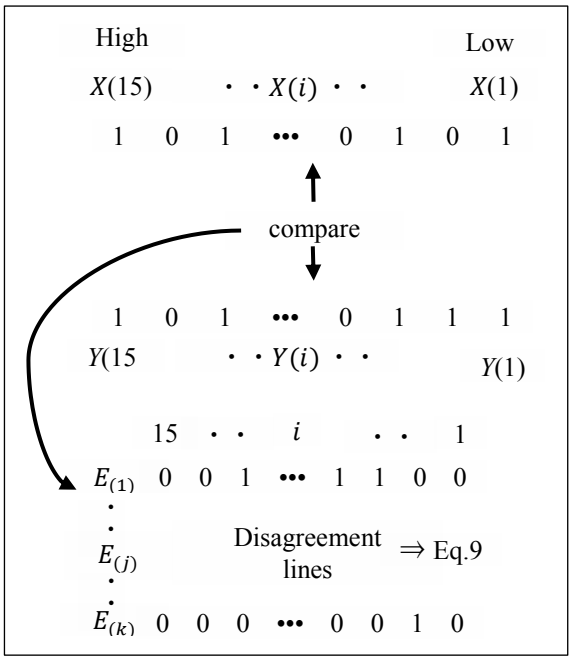


Fig. 10. Disagreement line compute model.

4. 計算機シミュレーション結果

4.1 シミュレーションシステム

Table 1 にシステムパラメータを示す. 伝搬特性の相互測定において同一周波数の送受信は TDD で行うが，標本間隔がフェージング変動周期に対して 1/10000 と非常に細かく設定したため正規局間の受

信時間誤差は無視できる程に小さくなる. そのため, 両局における相関の低下はほとんど無いものと考え, シミュレーションの簡易化のため両局間のフェージング変動周期は同一のものとする．また，観測ブロック長はフェージング変動周期の 10 倍の長さとした．レベル交差時刻情報検出のための基準値の設定方法については 3.4，3.5 節に準ずるものとする．

Table 1. System parameters.

Propagation channel	Two paths model Frequency selective fading Maximum Doppler:f_D[Hz] Delay time:1μsec
Transmitting system	Two waves transmission Bandwidth:1MHz Frequency difference:450kHz
Receiving system	Sampling interval:$1/f_D$ Measurement block:$10\times 1/f_D$ Smoothing:Band-pass filter $4f_D$[Hz] Derivation of phase difference
Key generartion	Station X : Setting of the standard value (=level) The transmission of the standard value Station Y: The reception of the standard value The detection of the level crossing time Common characteristic: Calculation of space data Encoding binary by space data

4.2 隣接標本値間の位相変動幅の出現確率と上限の設定

まず，基準値の設定可能領域を限定するための上限を設定する．その前段階として，標本値間の位相変動幅の出現確率についての評価を行った．特に下限の設定を大きくしすぎると設定可能領域が極端に狭くなってしまい，基準値の設定が困難となってしまう．そのため，ある程度出現確率の高い領域を含めて検討する必要がある．0~180 度の間を 1 度刻みの間隔でとった場合, 0~1 度の範囲ではほぼ 100%の出現確率であるが，1~2 度の範囲では 0.05%とほとんど出現せず，それ以降の範囲でもほとんど出現しない．そこで上限は 1 度と設定する．次に 0~1 度の範囲を 0.1 度刻み間隔でとった結果を Fig. 11 に示す. 0~0.1 度の範囲における確率は約 93%であったことから，少なくともこの領域は基準値の設定可能領域として含める必要がある.

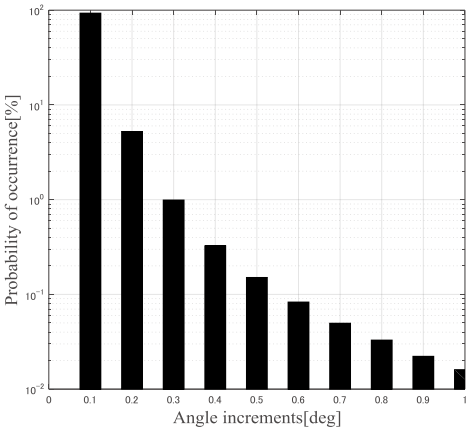


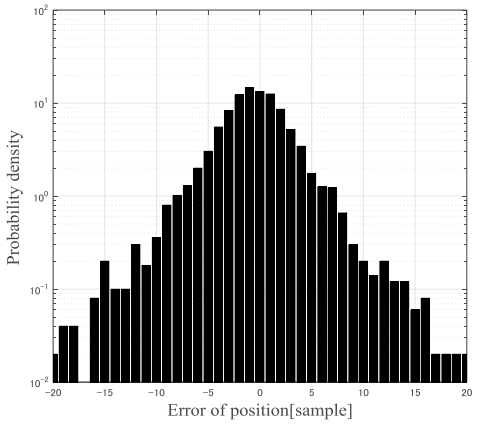
Fig. 11. Occurrence probability of angle increment. (0.1 degree increments).

4.3 標本値検出時刻の誤差特性

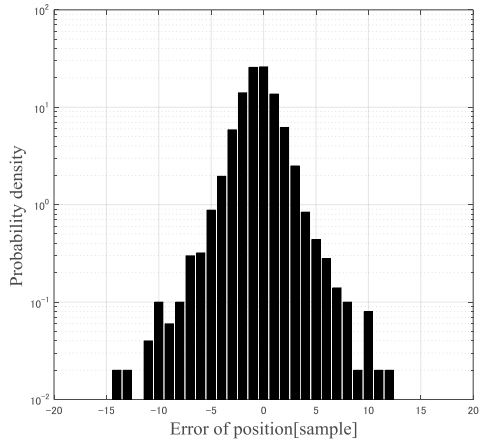
4.3.1 下限の決定と正規局間の検出誤差特性

続いて下限について検討する．標本値の検出はブロックごとに 1 サンプルとし，観測ブロック長が 10 ブロックであるため, その数は 10 サンプル程度となる. 3.4 節で記述したような信号強度の減衰領域の回避を実行しなかった場合における SN 比 30dB とした下限が 0.02 度の標本値検出時刻誤差特性を Fig. 12 の(a)に，下限 0.03 度の場合を(b)に示す．下限を 0.02 度と設定した場合での誤差は-20~20 サンプル程度であり，0.03 度では-15～15 サンプル程度である．したがって，傾きの急峻な観測領域から基準値を設定したほうが検出時刻誤差の低減がはかれることがわかる．続いて，信号強度の減衰領域の回避を実行した場合における下限を 0.02 度とした特性を Fig. 12 の(c)に，下限 0.03 度の場合を(d)に示す．どちらの下限においても減衰領域を回避することにより，回避しない場合と比較して誤差が低減されていることがわかる．ここで，図には示していないが下限の設定を 0.04 度した場合では，基準値を設定しないブロックも存在し，標本値検出時刻の取得確率は観測ブロック長に対して約 70%程度であった．また，反対に 0.01 度に設定した場合，ほぼ 100%で標本値の検出

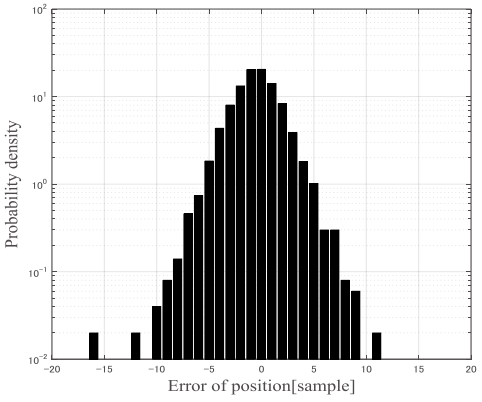
が行われるが，その時刻誤差は大きくなる．そのため下限を0.03度と設定することが適切であると判断した．



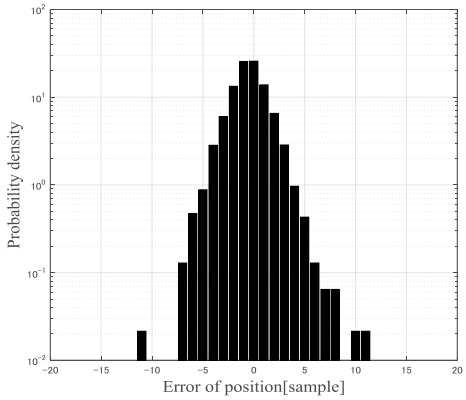
(a) Above 0.02 degree (before measure).



(b) Above 0.03 degree (before measure).



(c) Above 0.02 degree (after measure).



(d) Above 0.03 degree (after measure).

Fig. 12. Probability distribution of disagreement position.

4.3.2 正規-盗聴局間の特性

次に盗聴局における特性を評価する．SN 比を30dB，相関を 0.9 とした場合の標本値検出時刻の誤差特性を Fig. 13 に示す. Fig. 12 の正規局間の誤差と比較すると広い範囲で発生していることがわかる．

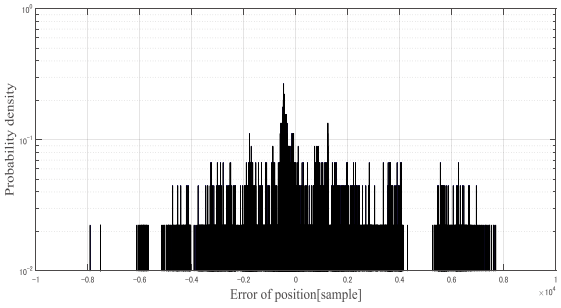


Fig. 13. Probability distribution of disagreement position.

4.4 正規局における各ビットの不一致率

まず, 3.6 節に基づいて正規局間における各 2 進符号化ビットの不一致率を Fig. 14 に表示する．下位ビット側では SN 比が低い環境において，不一致率は約 40～50%付近であり，SN 比が高くなるにつれてその不一致率は低下していることがわかる．特に第 1 ビットについてはどの SN 比に対しても 50%に近郊している．このことから，雑音の影響により検出時刻が多少でも異なれば，下位ビット側ではその影響を受けやすく，ビット誤りが発生しやすくなる．一方で，上位ビット側では SN 比が低い環境であっ

ても，不一致率が低いことがわかる．第 9 ビット以降に関しては不一致率が 10%を下回っており，約 90%以上の確率でビットが一致する．これより，上位ビット側では雑音の影響を受けにくくビット誤りは生じにくいため，秘密鍵生成に有効的なビットであると考えられる．

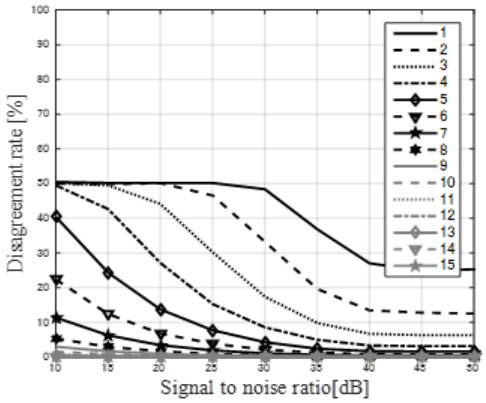


Fig. 14. Disagreement rate for each binary bit (Regular station).

4.5 盗聴局との各ビットの不一致率

次に正規-盗聴局間における各 2 進符号化ビットの不一致率の特性を相関係数 ρ として 0.9 の場合を Fig. 15 に示す．下位ビットから第 10 ビット程度までの不一致率は SN 比に関係なく約 50%で，最上位ビットに近づくにつれて不一致率は低下している．そのため半数程度の一致となるため盗聴は困難であると考えられる．しかし，第 11~15 ビットでの不一致率は低下しているため，相関が高くなるほど上位ビット側における正規局間で共有できる情報量が多くとも，盗聴される情報量が多くなるため，正味の情報量は少なくなる可能性がある．

4.6 各ビットの 2 進数の偏りの評価

正規局間において各 2 進符号化ビットの不一致率が低い場合であっても 2 進数の出現に偏りが生じ，盗聴局とも一致してしまうと秘密鍵容量は増加しない．そこで 2 進数の内の「0」になる確率を調査する．その出現の偏りについて正規局間の特性を Fig. 16 に，相関 0.9 とした正規-盗聴局間の特性を Fig. 17 に示す．

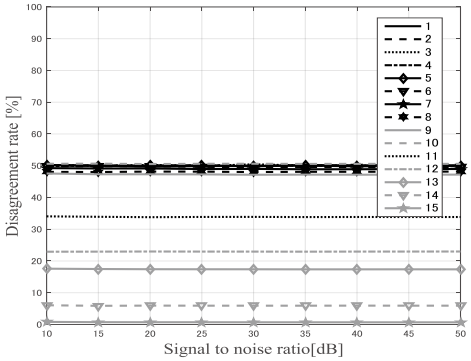


Fig. 15. Disagreement rate for each binary bit.

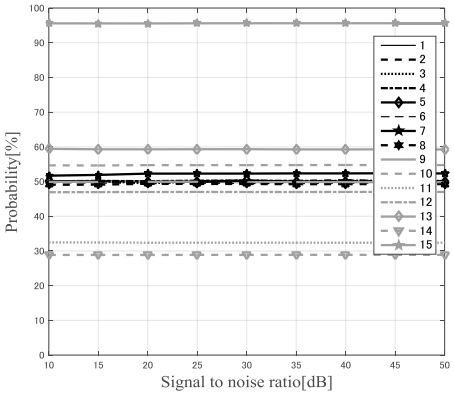


Fig. 16. Probability to become 0 of the each binary bit (Regular station).

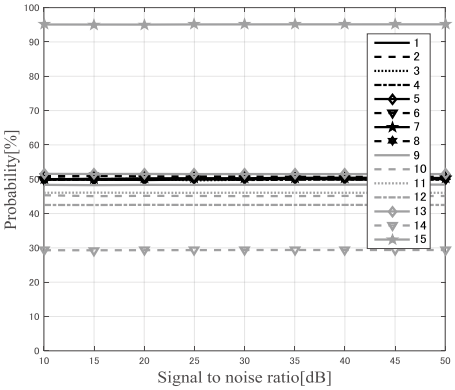


Fig. 17. Probability to become 0 of the each binary bit (Wiretapping station, ρ=0.9).

第 1~9 ビット程度の下位から中間ビットの確率は両局において約 50%で「0」と「1」の出現確率はほとんど変わらない．しかし，第 10 ビット以降の上位ビットでは最上位ビットに近づくにつれて 2 進数の

出現に偏りが生じ始めている．特に第 14，15 ビットでは両局間で出現確率に大きく偏りが生じている．このため，最上位ビットに近い上位ビットでは相互情報量が低下し，秘密鍵容量は少なくなることが見込まれるため，秘密鍵の生成には不適切なビットであると考えられる．

4.7　相互情報量・秘密鍵容量の評価

前節の結果より，各 2 進符号化ビットの特性は相互情報量や秘密鍵容量と密接に関係していることが考えられる．そこで本節では実際に各 2 進符号化ビットにおける相互情報量と秘密鍵容量について調査した結果を示す．

4.7.1 相互情報量特性

各ビットにおける正規局間の相互情報量についての結果を Fig. 18 に示す．

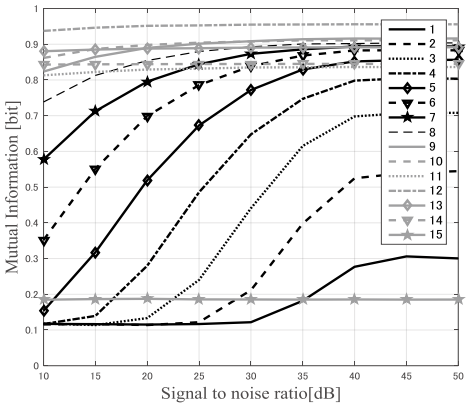


Fig. 18. Mutual Information for each binary bit (Regular station).

正規局間において，SN 比の低い環境では下位ビット側での共有できる相互情報量は少ないことがわかる．これは雑音の影響により間隔データに誤差が生じてしまうからである．しかし，雑音の影響が少ない SN 比の高い環境では 2 進数の不一致率が低くなることから，相互情報量が増加している．一方，第 13 ビット程度からは相互情報量が低下している．これは上位ビット側における 2 進数の不一致率は低い反面，その出現に偏りが生じるためであり，結果として相互情報量は低下する．以上より，下位ビットと上位ビットにおける相互情報量は少なくなり，それを除く中間ビットは 2 進数の出現のランダム性により相互情報量を持つことがわかる．

4.7.2　秘密鍵容量特性

4.7.1 節では 2 局間における相互情報量を評価した．以上の結果を踏まえ，盗聴局に知られず正規局間のみで共有できる秘密鍵容量についての評価を行った．Fig. 19 には生成した全ての秘密鍵に対する秘密鍵容量特性を示す．SN 比が 30dB における秘密鍵容量は約 0.5 ビットであり，1 つの間隔データから生成されるビットは 15 ビット程度である．観測ブロック長を $10\times1/f_{\mathrm{D}}$ としているが，ブロックによってはレベル交差時刻の検出を行わない．そのため標本値検出の平均サンプル数が約 9～10 サンプルとなるため，間隔データ数は 8~9 個程度となる．したがって，秘密鍵長は約 120～135 ビットとなる．以上より，共有できる秘密鍵容量は約 60~68 ビットとなる．

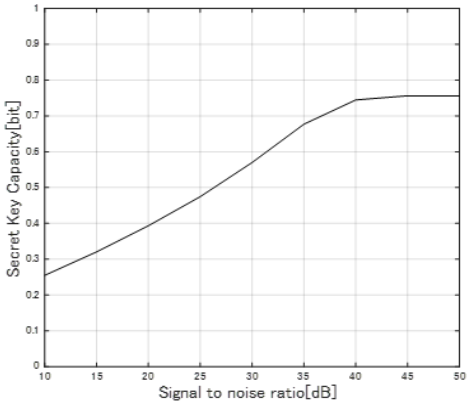


Fig. 19. Secret key capacity.

次に各 2 進符号化ビットにおける秘密鍵容量の結果を Fig. 20 に示す．SN 比が 30dB において，第 1 ビットから第 3 ビットの下位ビット側での秘密鍵容量は 0.5 ビットを下回っており，秘密鍵容量は少ない．一方，中間ビットから上位ビット側の第 4~12 ビットでは SN 比によらず 0.5 ビット程度以上であり，秘密鍵容量は多くなる．しかし，第 13~15 ビットのように最上位ビットの近傍の上位ビットでは，正規局間の相互情報量が高くとも盗聴局に盗聴されやす

いため，結果として秘密鍵容量は低下する．以上より，秘密鍵を生成するには中間ビットから最上位ビットの近傍の上位ビットまでを用いることが有効的であるとわかる．

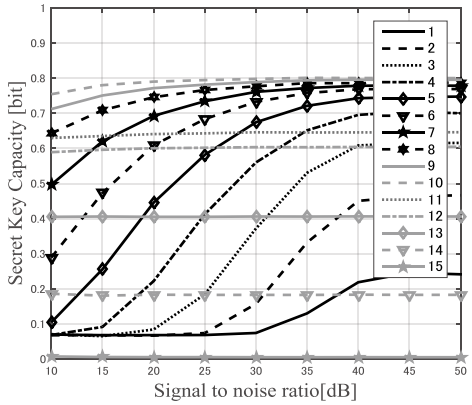


Fig. 20. Secret key capacity for each binary bit.

5. まとめ

本論文では，フェージングの位相変動，特に，絶対位相を容易に用いられることから位相差の時間変動に基づいてレベル交差時刻情報から秘密鍵を共有する方式を提案した．鍵の元となるビットは時刻間隔データを 2 進符号化することにより作成し，鍵生成に有効なビットを見定めるため，各ビットの秘密鍵容量や 2 進数の出現確率，不一致率についてシミュレーションにより評価を行った．

その結果，下位ビット側における秘密鍵容量は雑音の影響により正規局間でも 2 進数の不一致率は高くなるため少なくなる．その一方，上位ビット側では雑音の影響による 2 進数の不一致率は低くなるが，特に最上位ビット付近において，2 進数の出現の偏り方が下位ビット側と比較して，顕著に現れるため秘密鍵容量は低下していた．そのため，レベル交差時刻情報の間隔データを用いて秘密鍵を生成する場合には，適当なビットを選択する必要があるとわかった．また，本方式の場合において，生成した秘密鍵において盗聴局に知られず正規局間のみで共有できる情報量は SN 比 30dB において約 6 割を共有することができる．したがって，フェージングの位相変動に基づいて秘密鍵を生成することは可能であることがわかった．

本研究の一部は，科学研究費補助金基盤研究 (C) (課題本号 15K06091) の助成により実施した．

参考文献

1) 笹岡秀一，“電波伝搬を活用した情報理論的に安全な暗号方式”，電子情報通信学会技術研究報告，A･P 2007-**12**，65-70 (2007).
2) J. E. Hershey, A. A. Hassan, R. Yarlagadda, “Unconventional Cryptographic Keying Variable Management”, *IEEE Trans. Communi.*, **43**[1], 3-6 (1995).
3) 岩井誠人，笹岡秀一，“電波伝搬特性を活用した秘密情報の伝送･共有技術”，電子情報通信学会論文誌 B, **90**[9]，770-783 (2007).
4) 堀池元樹，笹岡秀一，“陸上移動通信路の不規則変動に基づく秘密鍵共有方式”，電子情報通信学会技術研究報告，RCS2002-**173**，7-12 (2002).
5) 松本達矢，笹岡秀一，岩井誠人，“公開通信路による乱数伝送と電波伝搬特性に基づく部分系列選択とを用いた秘密鍵共有方式の検討”，電子情報通信学会技術研究報告，RCS2015-192，13-18 (2015).
6) 西野太志，笹岡秀一，岩井誠人，“複数アンテナ送受信システムにおける電波伝搬特性に基づく秘密鍵共有方式”，電子情報通信学会技術研究報告，RCS2008-**275**，373-378 (2009).
7) 今井秀樹，情報理論，(昭晃堂，東京，2004).
8) 福田明，基礎通信工学，(森北出版，東京，2007).