漏えい鍵共有グラフにおける効果的な鍵選択に関する考察

増田 真吾[†1]　林 優一[†2]　水木 敬明[†3]　曽根 秀昭[†3]

概要：プレイヤーの幾つかの対が事前に 1 ビットの鍵を共有している状況をグラフで表現し，グラフの辺に対応するそれらの鍵はある確率分布に従い盗聴者 Eve に漏えいしているとする．このとき，特定の 2 人のプレイヤーが，他のプレイヤーと協力して，Eve への漏えい確率ができるだけ小さい 1 ビットの秘密鍵を共有したいとする．本稿では，完全グラフを仮定し，各鍵の漏えいが独立かつ等確率で起きる場合について，Eve への漏えい確率の最小値を解析的に求める．そのような最小値は，グラフのすべての鍵を使うときに実現できるが，すべての鍵を使わない場合の漏えい確率について考察し，効果的な鍵選択を検討する．

キーワード：情報漏えい，秘密共有法，鍵共有グラフ

1. はじめに

n人のプレイヤーと盗聴者 Eve がいて，プレイヤーの幾つかの対が事前に 1 ビットの鍵を共有しているとする．この状況を，各プレイヤーを点$v \in V$とし，鍵を共有しているプレイヤーの対を辺$e \in E$として得られるグラフ$G = (V, E)$で表現し，それを**鍵共有グラフ**と呼ぶ．各辺$e \in E$に対応する鍵の値を$k_e \in \{0,1\}$と書くことにする．これらの鍵は事前に何らかの方法（例えば，Diffie-Hellman 鍵交換，RSA 暗号，量子暗号，郵便，電子メールなど）で共有されており，ある確率分布に従って Eve に漏えいしていると仮定する．すなわち，漏えい辺集合$F \subseteq E$がある**漏えい分布**$\mathcal{L}$に従って生起し，その漏えい辺集合 F に含まれるすべての鍵の値が Eve に知られているとする（F に含まれない各鍵に対しては, Eve は$1/2$を超える確率でその値を当てられない）．このような鍵共有グラフGと漏えい分布$\mathcal{L}$の対$(G, \mathcal{L})$を**部分的漏えい鍵共有グラフ**と呼ぶ．

いま, 例として図 1 に示すような$n = 3$のときの鍵共有グラフG^{ex}を考えよう．

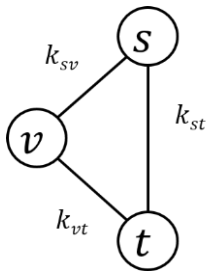


図 1　鍵共有グラフ$G^{ex} = (\{s, t, v\}, \{st, sv, vt\})$

このグラフG^{ex}は，プレイヤーsとt，sとv，vと t がそれぞれ 1 ビットの鍵k_{st}, k_{sv}, k_{vt}を共有していることを示している．べき集合$2^{\{st,sv,vt\}}$の上に確率分布を与えることで，漏えい分布を定めてみよう．もし各鍵の漏えいが独立に発生していて，その漏えい確率が等しく0.1であるとすると，その漏えい分布$\mathcal{L}_1$は表 1 のようになる．

表 1　漏えい分布$\mathcal{L}_1$

漏えい辺集合	$\{k_{st}, k_{sv}, k_{vt}\}$	$\{k_{st}, k_{sv}\}$	$\{k_{st}, k_{vt}\}$
発生確率	0.001	0.009	0.009

$\{k_{sv}, k_{vt}\}$	$\{k_{st}\}$	$\{k_{sv}\}$	$\{k_{vt}\}$	$\emptyset$
0.009	0.081	0.081	0.081	0.729

この漏えい分布$\mathcal{L}_1$の例では各鍵の漏えいは独立に発生していたが，一般には各鍵の漏えいは必ずしも独立であるとは限らない．例えば，鍵共有グラフG^{ex}に対して，表 2 の漏えい分布$\mathcal{L}_2$のように, 確率0.1ですべての鍵が漏えいし, 確率0.2で鍵k_{st}のみが漏えいし，確率0.7ですべての鍵が漏えいしないという場合も考えられる（それ以外の漏えい辺集合の発生確率は 0 である）．

表 2　漏えい分布$\mathcal{L}_2$

漏えい辺集合	$\{k_{st}, k_{sv}, k_{vt}\}$	$\{k_{st}\}$	$\emptyset$
発生確率	0.1	0.2	0.7

いま，部分的漏えい鍵共有グラフとして 2 つの例$(G^{ex}, \mathcal{L}_1)$と$(G^{ex}, \mathcal{L}_2)$を見た．本研究では，部分的漏えい鍵共有グラフ$(G, \mathcal{L})$とGに含まれる 2 人のプレイヤーs，tが与えられたとき，他のプレイヤーと協力して，s，t間でできるだけ Eve への漏えい確率が小さい 1 ビットの秘密鍵$u \in \{0,1\}$を共有したいという問題を考える．このとき，uの値が他のプレイヤーに知られるのは構わないとする．

例えば，部分的鍵共有グラフ$(G^{ex}, \mathcal{L}_1)$において，プレイヤーsとtが既に共有している鍵k_{st}をそのまま目的の秘密鍵uとして用いるプロトコル$\wp_1$を考えると, uの Eve への漏えい確率は，もちろん0.1である．このことを，

$$\mathcal{E}_{\wp_1}(G^{ex}, \mathcal{L}_1) = 0.1$$

のように書く．

†1 東北大学　情報科学研究科
†2 東北学院大学　工学部
†3 東北大学 サイバーサイエンスセンター

別な例として鍵k_{sv}とk_{vt}を使うプロトコル$\wp_2$を考えよう．プレイヤーsがランダムにビットuを選び，k_{sv}をワンタイムパッド[3]として用い，uを暗号化してプレイヤーvに送る．受け取ったvは同様にしてuをプレイヤーtに送る．これによりsとtは 1 ビットの秘密鍵uを共有することができ，Eve がuを知るのは，鍵k_{sv}とk_{vt}の内少なくとも一つの鍵が漏えいしているときに起こるので，

$$\mathcal{E}_{\wp_2}(G^{ex}, \mathcal{L}_1) = 1 - (1 - 0.1)^2 = 0.19$$

となる．（なお，プレイヤーvは秘密鍵uを知ってしまうが，上述のとおり構わない．）

上の 2 つのプロトコル$\wp_1$と$\wp_2$を組み合わせて 3 つの鍵すべてを使うこともできる．すなわち，プロトコル$\wp_1$で秘密鍵u_1を sとtで共有し，さらにプロトコル$\wp_2$で秘密鍵u_2を共有する．sとtはそれぞれ$u_1 \oplus u_2$を計算し目的の秘密鍵とすることができる．これをプロトコル$\wp_3$と呼ぶと，Eve への漏えい確率は，

$$\mathcal{E}_{\wp_3}(G^{ex}, \mathcal{L}_1) = 0.019$$

となる．

これら 3 つのプロトコルを有向辺を用いて図示すると，図 2 のようになる．

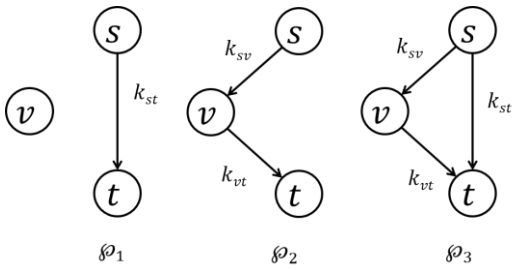


図 2　プロトコル$\wp_1, \wp_2, \wp_3$の模式図

この 3 つ例の中で Eve への漏えい確率が最も小さいのは，すべての鍵を用いるプロトコル$\wp_3$である．実際，すべての鍵を用いる st-フロープロトコル[1]が知られており（$\wp_3$は$(G^{ex}, \mathcal{L}_1)$に対する st-フロープロトコルになっている），これを用いるとどんな部分的漏えい鍵共有グラフにおいても Eve への漏えい確率を最小にできることが証明されている（2.1 節で詳しく説明する）．

一方で，st-フロープロトコルは鍵共有グラフのすべての鍵を使い切ってしまうという問題があり，「漏えい確率は最小にしなくても良いので鍵を全部使わず次回の秘密共有のために少し残しておきたい」という場合に対応できない．例えば，上の例において，3 本の鍵を用いるプロトコル$\wp_3$のように0.019まで Eve への漏えい確率を下げなくても，1 本の鍵を用いるプロトコル$\wp_1$で得られる漏えい確率0.1で十分な場合もある．しかも上で見たように， 2 本の鍵を用いることが 1 本だけの場合より Eve への漏えい確率を必ずしも下げられるとは限らない．従ってどのように鍵を選択するかは極めて重要な問題である．

任意の部分的漏えい鍵共有グラフに対して，上述の鍵選択に関する問題を解決することは難しいように思われるので，既存研究[2]では，鍵共有グラフが完全グラフであり，等しい確率pで各鍵が独立に漏えいする**一様漏えい鍵共有完全グラフ**を仮定している．この一様漏えい鍵共有完全グラフに対して，$l \leq 2n - 3$を満たすl本の鍵を用いるとした場合の最適な鍵選択を行う手法が提案されており，尚且つ Eve への漏えい確率の値が解析的に求まっている（2.2 節で詳しく説明する）．

n点の完全グラフは$(n^2 - n)/2$本の辺を持つので，この値が選べる鍵の総数となる．上述の既存研究[2]は$2n - 3$本までの鍵の選び方しか示唆しないので，残りの$(n^2 - 5n + 6)/2$本の鍵をどのように選べばよいかは未解決である．上述したように残り$(n^2 - 5n + 6)/2$本をすべて使い切る st-フロープロトコル[1]を用いれば Eve への漏えい確率を最小にできるが，その値を解析的に求めることは未解決であるため，$2n - 3$本までの鍵を用いる方法と比べてどれだけ効果的であるかも不明である．

そこで本研究では，一様漏えい鍵共有完全グラフに対して st-フロープロトコルがすべての鍵を用いることで得られる Eve への漏えい確率の最小値を解析的に求めることを目的とする．すなわち，漏えいが発生する条件をグラフ理論に基づき場合分けし，Eve の漏えい確率の最小値を与える漸化式を示す．これにより，$2n - 3$本までの鍵を用いる方法と比べ Eve への漏えい確率がどれだけ下がるのかを容易に計算できるようになるので，消費する鍵数とのトレードオフを考慮して効果的な鍵選択を行えることが期待できる．実際，典型的な場合について計算を行い，どのような鍵選択を行えば効果的な鍵選択となるかについて，可視化を与える．

上で見たように，本稿では，鍵共有グラフの存在を仮定して，それを利用して秘密鍵の共有を行う問題を扱っている．各プレイヤーは，事前知識として鍵共有グラフで示される鍵のみを知っており，それ以降の他のプレイヤーとの通信は，盗聴者 Eve も含めてすべてのプレイヤーへ同報されるものとしている．このような状況を仮定している既存研究には文献[4][5]がある．一方，鍵共有グラフを仮定するのではなく，部分的な通信路を仮定して秘密伝送（Secure Message Transmission や Private Message Transmission）を実現する研究も数多く存在している（例えば文献[6]）．本稿における設定では，あくまでも通信路は公衆回線である，すなわちすべてのメッセージは同報されることに注意されたい．

本稿の構成は次の通りである．まず 2 章では，st-フロープロトコル[1]と一様漏えい鍵共有完全グラフを仮定した既存研究[2]について説明する．次に 3 章では，Eve への漏えい確率の最小値を解析的に求めるための漸化式を提案する．その漸化式に基づき 4 章で効果的な鍵選択に関する考察を行う．最後に 5 章でまとめを行う．

2. 既存研究

本章では，まず 1 章で取り上げた問題を解決する方法として知られている st-フロープロトコル[1]について説明を行う．次に一様漏えい鍵共有完全グラフに対して，$l \leq 2n-3$を満たすl本の鍵を用いるプロトコル[2]について説明を行う．

2.1 st-フロープロトコル

st-フロープロトコル[1]は，“st-numbering”に基づき有向グラフを作り，1 章で述べたように，すべての鍵を使い共有される秘密鍵uの Eve への漏えい確率を最小にする．すなわち，任意の部分的漏えい鍵共有グラフ$(G,\mathcal{L})$が与えられたとき，どんなプロトコル$\wp$に対しても

$$\mathcal{E}_{\wp}(G,\mathcal{L}) \geq \mathcal{E}_{\text{st-flow}}(G,\mathcal{L})$$

である（st-flow は st-フロープロトコルを表す）．

また，秘密鍵uが Eve へ漏えいするかしないかについては，漏えい辺集合のグラフ理論的性質によって特徴づけられることが知られている．具体的には，図 3 のように漏えい辺集合Fがsとtを分離するとき（**カット**であるとき），Eve に秘密鍵uが漏えいする．図 4 のように漏えい辺集合Fがsとtを分離しないとき，Eve に秘密鍵uが漏えいしない．

従って，$G=(V,E)$なる部分的漏えい鍵共有グラフ$(G,\mathcal{L})$に対し，sとtを分離する漏えい辺集合の集合を

$$Sep(s,t;G) = \{F \subseteq E | F \text{は} s \text{と} t \text{を分離}\}$$

と定義し，$\Pr(F)$を漏えい辺集合Fが生起する確率とすると，次の定理が成立する．

定理 1([1]) $(G,\mathcal{L})$を任意の部分的漏えい鍵共有グラフとする．任意のプロトコル$\wp$に対して，

$$\mathcal{E}_{\wp}(G,\mathcal{L}) \geq \mathcal{E}_{\text{st-flow}}(G,\mathcal{L}) = \sum_{F \in Sep(s,t;G)} \Pr(F)$$

が成り立つ．

しかしながら，

$$\sum_{F \in Sep(s,t;G)} \Pr(F)$$

の値を解析的に求める方法は知られていない．

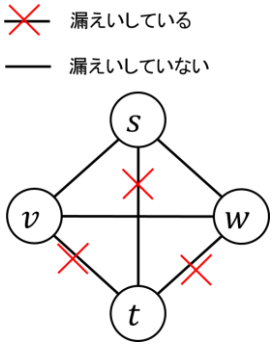


図 3　sとtを分離している

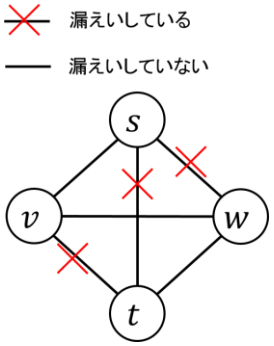


図 4　sとtを分離していない

2.2 一様漏えい鍵共有完全グラフに対する既存研究

既存研究[2]では，部分的漏えい鍵共有グラフ$(G,\mathcal{L})$として，一様漏えい鍵共有完全グラフを仮定している．すなわち，p $(0 \leqq p \leqq 1)$を固定し，各鍵は独立に確率pで漏えいし，Gは完全グラフK_nであると仮定する．このような一様漏えい鍵共有完全グラフを(K_n,p)と書くことにする．

無論，一様漏えい鍵共有完全グラフ(K_n,p)に対しても st-フロープロトコル[1]は Eve への漏えい確率を最小にする．しかしながら，すべての鍵を使い切ってしまうという問題がある．そこで既存研究[2]では，$2n-3$本までの鍵の最適な選び方を提案している．具体的には，$l \leq 2n-3$なるl本の鍵を用いたプロトコル$\wp^{l}_{\text{path}}$を次のように与えている．

1. 辺stを選択する
2. 選択した辺の合計がlを超えない限り，sとtを結ぶ長さ 2 の道を構成する 2 辺を選択する（図 5 参照）
3. lが 6 以上の偶数のときはs，tを除く点同士を結ぶ 1 辺を選択する（図 6 参照）

このプロトコル$\wp^{l}_{\text{path}}$の漏えい確率は，次の補題のように計算できる．

補題 1（[2]） (K_n,p)を任意の一様漏えい鍵共有完全グラフとし，$l \leq 2n-3$とする．lが奇数のとき，

$$\mathcal{E}_{\wp^{l}_{\text{path}}}(K_n,p) = p(2p-p^2)^{\frac{l-1}{2}}$$

であり，lが 6 以上の偶数のとき，

$$\mathcal{E}_{\wp^{l}_{\text{path}}}(K_n,p) = p(2p^5-5p^4+2p^3+2p^2)(2p-p^2)^{\frac{l-6}{2}}$$

である．また，$\mathcal{E}_{\wp^{2}_{\text{path}}}(K_n,p) = p$であり，$\mathcal{E}_{\wp^{4}_{\text{path}}}(K_n,p) = p(2p-p^2)$である．

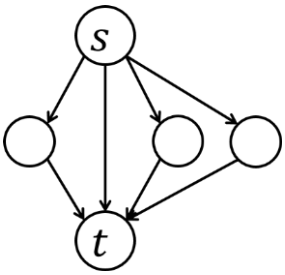


図 5　ステップ 2 までの$\wp^{l}_{\mathbf{path}}$の動作

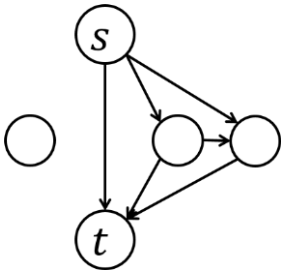


図 6　ステップ 3 までの$\wp^{l}_{\mathbf{path}}$の動作

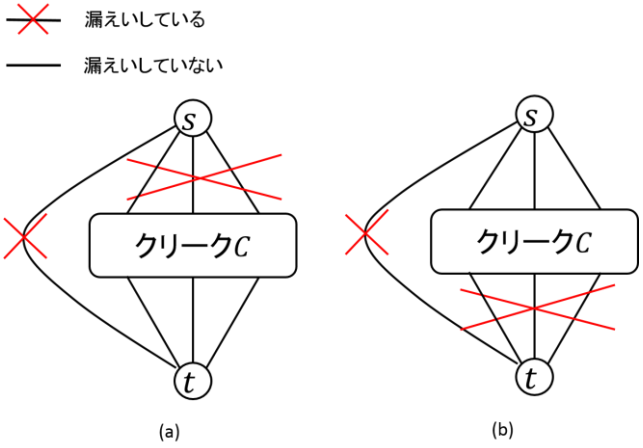
3. 最小値$\mathcal{E}_{\mathbf{st-flow}}$を与える漸化式の算出

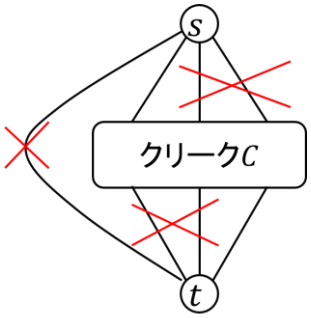
2.1 節で説明した st-フロープロトコルについて，Eve への漏えい確率$\mathcal{E}_{\mathrm{st-flow}}(G,\mathcal{L})$を解析的に求める方法が明らかでないという問題があった．そこで本章では，$(G,\mathcal{L})$を一様漏えい鍵共有完全グラフと仮定したとき，$\mathcal{E}_{\mathrm{st-flow}}(K_n,p)$を求める漸化式の提案を行う．

3.1 基本アイデア

定理 1 に述べたように，$\mathcal{E}_{\mathrm{st-flow}}(K_n,p)$の値は漏えい辺集合が$s$と$t$を分離する事象の確率$\sum_{F\in Sep(s,t;G)}\Pr(F)$に等しい．このような事象が発生するのはどのような場合であろうか？

n点の完全グラフGにおいて，sとtを除く$n-2$点のクリークをCとすると，漏えい辺集合がsとtを分離する事象は図 7 に示す 3 通りに分類できる．





(c)

図 7　漏えい辺集合がsとtを分離する事象

すなわち，まず辺stはどの場合においても漏えいしなくてはならない．その上で，図 7 の(a)のようにsとクリークCが分離される場合はsとtも分離される．図 7 の(b)のようにtとクリークCが分離される場合も同様である．図 7 の(c)のように，sとクリークC，tとクリークCが分離されていない場合，漏えい辺集合がsとtを分離するにはクリークCの中で分離される必要がある．

クリークCの中で分離される事象について詳しく説明する．まず，クリークCの内部に互いに素な 2 つのクリーク，クリークDとクリークEが存在し，クリークDとs，クリークEとtの間に少なくとも 1 本は漏えいしていない辺が存在しているとする（図 8 参照）．このとき，クリークDとクリークEを漏えい辺集合により分離することが図 7（c）の事象である．

従って，互いに素な 2 つのクリークを漏えい辺集合が分離する事象とその起きる確率を再帰的に考えると良さそうある．そこで$(a+b+k)$点の完全グラフにおいて，互いに素なa点クリークとb点クリークを考え，漏えい辺集合がそれらを分離する確率を$z(a,b;k)$と書くことにする（$a,b\geq 1$）．例えば，図 8 においてクリークC，D，Eがそれぞれc，d，e点で構成されているとすると，クリークDとEを漏えい辺集合が分離する確率は$z(d,e;c-d-e)$である．

st-フロープロトコルを用いた際の Eve への漏えい確率$\mathcal{E}_{\mathrm{st-flow}}(K_n,p)$は 2 つの 1 点クリーク（すなわち，点$s$と$t$）を分離する確率であるので，次のように与えられる．

$$\mathcal{E}_{\mathrm{st-flow}}(K_n,p)=z(1,1;n-2)$$

以降で$z(a,b;k)$を再帰的に求めていく．

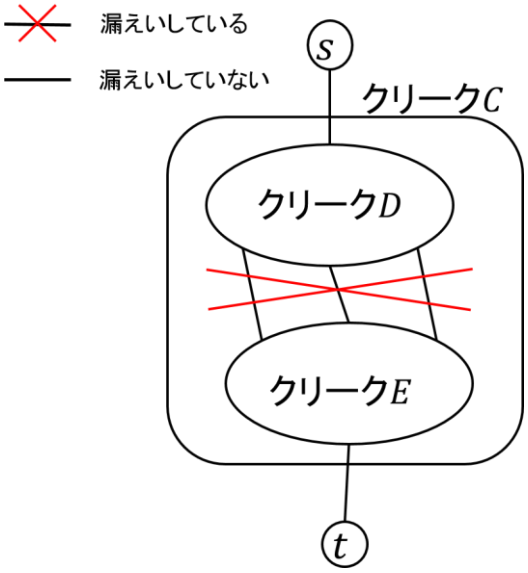


図 8　図 7（c）のクリークC

3.2 漏えい辺集合が 2 つのクリークを分離する条件

$(a+b+k)$点の完全グラフにおいて，互いに素なa点クリークとb点クリークを考える．このとき，これら 2 つのクリークを漏えい辺集合が分離する事象は，次の事象H_1が起き，かつ同時に事象H_a，事象H_b，事象H_cのいずれかが起きるときである．すなわち，

$$\mathrm{H}_1 \cap (\mathrm{H}_a \cup \mathrm{H}_b \cup \mathrm{H}_c)$$

である．

事象H_1：a点クリークとb点クリークを結ぶすべての辺が漏えいしている．

事象H_a：a点クリークとk点クリークを結ぶ辺がすべて漏えいしている．

事象H_b：b点クリークとk点クリークを結ぶ辺がすべて漏えいしている．

事象H_c：事象H_a，事象H_bが起こらず，漏えい辺集合がa点クリークとb点クリークを分離する．

なお，$(\mathrm{H}_a \cup \mathrm{H}_b) \cap \mathrm{H}_c = \emptyset$であるので，

$$\mathrm{H}_1 \cap (\mathrm{H}_a \cup \mathrm{H}_b \cup \mathrm{H}_c) = \mathrm{H}_1 \cap ((\mathrm{H}_a \cup \mathrm{H}_b) + \mathrm{H}_c)$$

と書けることに注意しよう．

3.3 各事象が起きる確率

ここでは，各事象が起きる確率を計算する．

(1) 事象H_1が起きる確率

図 9 の例のように，a点クリークとb点クリークを結ぶ鍵はab本存在する．よって，事象H_1が起きる確率は$\Pr[\mathrm{H}_1] = p^{ab}$と与えられる．

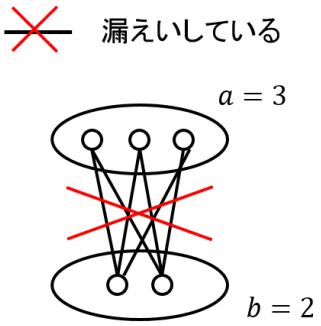


図 9　事象H_1の例

(2) 事象H_aと事象H_bが起きる確率

図 10 の例のように，事象H_aが起きる確率は$\Pr[\mathrm{H}_a]=p^{ak}$と与えられ，同様に，事象H_bが起きる確率は$\Pr[\mathrm{H}_b]=p^{bk}$と与えられる．よって，これらの事象の内少なくとも 1 つの事象が起きる確率は，$\Pr[\mathrm{H}_a \cup \mathrm{H}_b]$であり，次式で与えられる．

$$\Pr[\mathrm{H}_a \cup \mathrm{H}_b] = p^{ak} + p^{bk} - p^{(a+b)k}$$

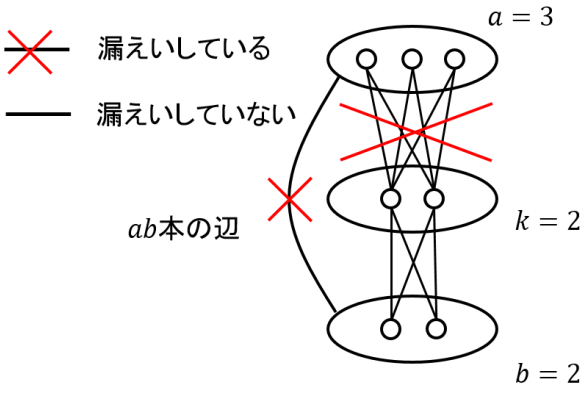


図 10　事象H_aの例

(3) 事象H_cが起きる確率

事象H_cは，図 11 のように，k点クリーク中に互いに素な 2 つのクリークIとJが存在し，次の 3 つの条件すべてを同時に満たすときに起こる．

条件 1：クリークI中の各点と，a点クリークは分離されず，k点クリーク中のそれ以外の点とa点クリークは分離される．

条件 1 が起きる確率は，クリークIの点数をiとすると，

$$(1-p^a)^i p^{a(k-i)}$$

で与えられる．

条件 2：クリークJ中の各点と，b点クリークは分離されず，k点クリーク中のそれ以外の点とb点クリークは分離される．

条件 2 が起きる確率は，クリークJ中の点数をjとすると，

$$(1-p^b)^j p^{b(k-j)}$$

で与えられる．

条件 3：クリークIとクリークJが分離される．

条件 3 が起きる確率は，クリークI中の点数をi，クリークJ中の点数をjとすると，

$$z(i,j;k-i-j)$$

で与えられる．

以上により，k点クリークから互いに素な 2 つのクリークIとJを選ぶ組み合わせを考慮すると，事象$\mathrm{H_c}$が起きる確率$\Pr[\mathrm{H_c}]$は次式で与えられる．

$$\Pr[\mathrm{H_c}] = \sum_{i=1}^{k-1}\sum_{j=1}^{k-i}\binom{k}{i}\binom{k-i}{j}(1-p^a)^i p^{a(k-i)}$$

$$(1-p^b)^j p^{b(k-j)} z(i,j;k-i-j)$$

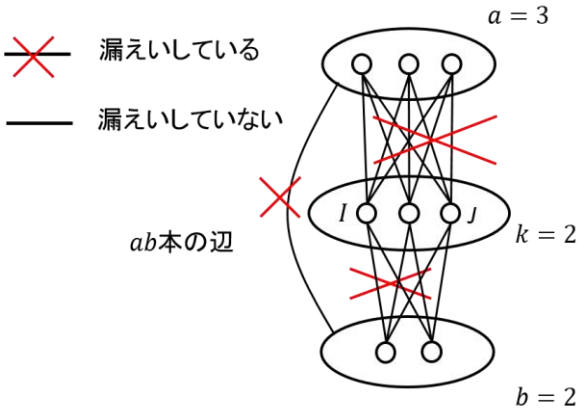


図 11　事象$\mathrm{H_c}$の例

これらをまとめると，クリークを分離するという事象$\mathrm{H_1} \cap (\mathrm{H_a} \cup \mathrm{H_b} \cup \mathrm{H_c})$が発生する確率，すなわち，

$$\Pr[\mathrm{H_1} \cap (\mathrm{H_a} \cup \mathrm{H_b} \cup \mathrm{H_c})]$$

は，次の定理で与えられる．

定理 2　$(a+b+k)$点（$a,b \geq 1$）の完全グラフにおいて，互いに素なa点クリークとb点クリークを漏えい辺集合が分離する確率$z(a,b;k)$は，次の漸化式を満足する．

（1）$k=0$の場合

$z(a,b;0) = p^{ab}$

（2）$k=1$の場合

$z(a,b;1) = p^{ab}(p^a + p^b - p^{a+b})$

（3）$k>1$の場合

$$z(a,b;k) = p^{ab}\{p^{ak}+p^{bk}-p^{(a+b)k} + \sum_{i=1}^{k-1}\sum_{j=1}^{k-i}\binom{k}{i}\binom{k-i}{j}(1-p^a)^i p^{a(k-i)} (1-p^b)^j p^{b(k-j)} z(i,j;k-i-j)\}$$

この定理により，$\mathcal{E}_{\mathrm{st-flow}}(K_n,p) = z(1,1;n-2)$の算出が可能となる．例として，$n=4$の場合，すなわち，$\mathcal{E}_{\mathrm{st-flow}}(K_4,p) = z(1,1;2)$について考えてみよう．定理 2 の（3）より，

$$z(1,1;2) = p(p^2+p^2-p^4+2(1-\mathrm{p})p(1-\mathrm{p})pz(1,1;0)) = p(2p^2-p^4+(2p^2-4p^3+2p^4)z(1,1;0))$$

定理 2 の（1）より，$z(1,1;0)=p$であるから，

$$z(1,1;2) = p(2p^2-p^4+2p^3-4p^4+2p^5) = 2p^3+2p^4-5p^5+2p^6$$

以上のように，$\mathcal{E}_{\mathrm{st-flow}}(K_4,p)$を各鍵の漏えい確率$p$の多項式で与えることができたので，具体的な値を$p$に代入することによって，共有される秘密鍵$u$の漏えい確率を容易に求めることができるようになった．

3.4　多項式の例

3.3 節で示した漸化式を利用して，もちろん$n=4$以外の場合も$\mathcal{E}_{\mathrm{st-flow}}(G,\mathcal{L})$を示す多項式を得ることができる．以下に$n=4$から$n=10$までの多項式を示す．

$$\mathcal{E}_{\mathrm{st-flow}}(K_4,p) = 2p^3+2p^4-5p^5+2p^6$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_5,p) = 2p^4+6p^6-7p^7-12p^8+18p^9-6p^{10}$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_6,p) = 2p^5+8p^8-3p^9-44p^{11}+20p^{12}+78p^{13}-84p^{14}+24p^{15}$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_7,p) = 2p^6+10p^{10}-11p^{11}+20p^{12}-70p^{14}-80p^{16}+340p^{17}-570p^{19}+480p^{20}-120p^{21}$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_8,p) = 2p^7+12p^{12}-13p^{13}+30p^{15}+20p^{16}-102p^{17}+72p^{18}-190p^{19}-150p^{20}+420p^{21}+110p^{22}+1380p^{23}-2700p^{24}-1050p^{25}+4680p^{26}-3240p^{27}+720p^{28}$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_9,p) = 2p^8+14p^{14}-15p^{15}+42p^{18}-70p^{20}+98p^{21}-322p^{23}-462pp^{24}+1050p^{25}-1456p^{26}+1680p^{27}+2940p^{28}-2030p^{29}+420p^{30}-19530p^{31}+21840p^{32}+18480p^{33}-42840p^{34}+25200p^{35}-5040p^{36}$$

$$\mathcal{E}_{\mathrm{st-flow}}(K_{10},p) = 2p^9+16p^{16}-17p^{17}+56p^{21}-184p^{23}+240p^{24}+70p^{25}-504p^{27}-392p^{28}+812p^{29}-840p^{30}-1736p^{31}+2464p^{32}+6314p^{33}-11424p^{34}+24304p^{35}-10640p^{36}-36260p^{37}-43680p^{39}+263760p^{40}-172200p^{41}-272160p^{42}+433440p^{43}-221760p^{44}+40320p^{45}$$

4. 効果的な鍵選択に関する考察

本章では，2 つのプロトコル，すなわち st-フロープロトコルとプロトコル$\wp^{l}_{\mathrm{path}}$について比較し，状況に応じてどちらのプロトコルが効果的な鍵選択であるかの考察を行う．以下の考察において，Eve への漏えい確率の目標値を定める意図はなく，あくまでもユーザーが鍵選択を行う際の指標となることを意識している．

4.1 既存研究[2]が有効な場合

本節では，プロトコル$\wp^{l}_{\mathrm{path}}$で十分であると考えられる場合について考察する．

例として，$p = 0.5$，$n = 10$のときの使用する辺（鍵）の本数に対する$\mathcal{E}_{\wp^{l}_{\mathrm{path}}}(K_{10}, 0.5)$の値（$l$は奇数）と$\mathcal{E}_{\mathrm{st-flow}}(K_{10}, 0.5)$を表示したグラフを図 12 に示す．図 12 の通り，$\mathcal{E}_{\wp^{l}_{\mathrm{path}}}(K_{10}, 0.5)$の最小値はおよそ 0.050056 であり，$\mathcal{E}_{\mathrm{st-flow}}(K_{10}, 0.5)$はおよそ 0.004037 である．これら 2 つの値を比較した際，使用する鍵の本数に対して Eve への漏えい確率に大きな減少は見られない．よって，このような場合はプロトコル$\wp^{l}_{\mathrm{path}}$が効果的であるといえる．

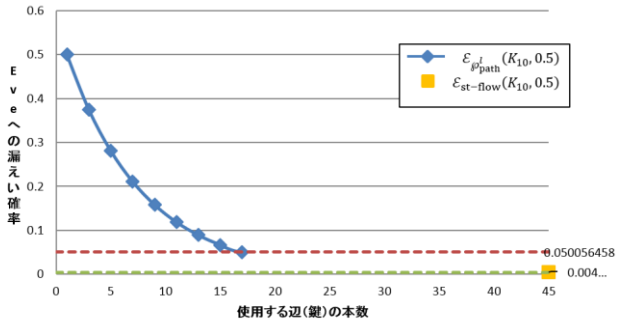


図 12　$p = 0.5$，$n = 10$のときの漏えい確率の推移

4.2 st-フロープロトコルが有効な場合

本節では鍵を最大まで使うことが効果的であると考えられる場合について考察する．

例として，$p = 0.7$，$n = 10$のときの使用する辺（鍵）の本数に対する$\mathcal{E}_{\wp^{l}_{\mathrm{path}}}(K_{10}, 0.7)$の値（$l$は奇数）と$\mathcal{E}_{\mathrm{st-flow}}(K_{10}, 0.7)$を表示したグラフを図 13 に示す．図 13 の通り，$\mathcal{E}_{\wp^{l}_{\mathrm{path}}}(K_{10}, 0.7)$の最小値はおよそ 0.329177 であり，$\mathcal{E}_{\mathrm{st-flow}}(\boldsymbol{K}_{10}, 0.7)$はおよそ 0.101662 である．これら 2 つの値を比較した際，Eve への漏えい確率におよそ 0.227515 の減少が見られる．これは，$p = 0.5$の場合の 2 つのプロトコル漏えい確率の差（0.046019）と比べて大きな値であると言えよう．よって，このような場合は st-フロープロトコルが効果的であると考えることもできる．

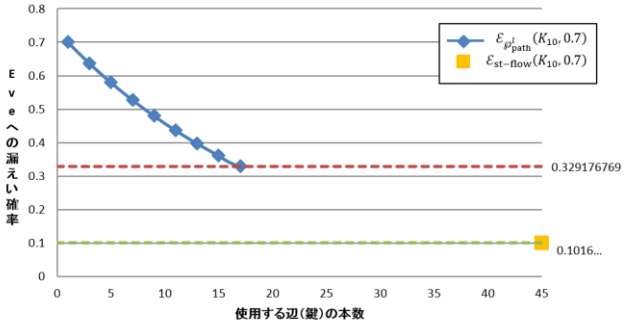


図 13　$p = 0.7$，$n = 10$のときの漏えい確率の推移

5. おわりに

一様漏えい鍵共有完全グラフに対して適切な鍵選択を行う為の基盤として，Eve への漏えい確率の最小値を求める漸化式を示し，効果的な鍵選択を行うための考察を行った．

今後の課題として，完全グラフ以外の鍵共有グラフやより一般の漏えい分布に対して，効果的な鍵選択を行う手法を検討することが挙げられる．また，ユーザーが Eve への漏えい確率と消費する鍵とのトレードオフをより理解できるように適切な指標を与えることも重要である．さらに，本稿では，sとt以外の他のプレイヤーにも秘密鍵uの値が知られてもよいと仮定しているが，そのような仮定をおかない研究の方向も望まれる．例えば，st-フロープロトコルでもプロトコルプロトコル$\wp^{l}_{\mathrm{path}}$でも，選択された鍵が二連結グラフを構成している場合には，結託が起きない限り，他のプレイヤーにuの値が知られることはない．

参考文献

[1] Takaaki Mizuki, Satoru Nakayama, and Hideaki Sone, “An application of st-numbering to secret key agreement, ” International Journal of Foundations of Computer Science, vol.22, no.5, pp.1211-1227, 2011.

[2] 松田重裕，林優一，水木敬明，曽根秀昭, “部分的鍵共有グラフにおける鍵選択関する一考察, ” 電子情報通信学会総合大会情報・システム論文集 1, p.5, 2012.

[3] G.S.Vernam, “Cipher printing telegraph systems for secret wire and radio telegraphic communications, ” Journal of the American Institute for Electrical Engineers, vol.55, pp.109–115, 1926.

[4] Takaaki Mizuki, Takuya Sato, and Hideaki Sone, “A One-Round Secure Message Broadcasting Protocol through a Key Sharing Tree, ” Information Processing Letters, vol.109, no.15, pp.842-845, 2009.

[5] Yoshihiro Indo, Takaaki Mizuki, and Takao Nishizeki, “ Absolutely Secure Message Transmission Using a Key

Sharing Graph, ” Discrete Mathematics,Algorithms and Applications, vol.4, no.4, 1250053 (15 pages), 2012.

[6] Hadi Ahmadi and Reihaneh Safavi-Naini, “Private Message Transmission Using Disjoint Paths, ” Applied Cryptography and Network Security, Lecture Notes in Computer Science, vol.8479, pp. 116-133, 2014.