ISS-P-131

一様漏えい鍵共有完全グラフに対する二者鍵共有の限界

増田　真吾† 林　優一†† 水木　敬明† 曽根　秀昭†
† 東北大学大学院情報科学研究科　　†† 東北学院大学工学部

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ビットの秘密鍵を共有しているとする．この状況を，各プレイヤー $v \in V$ を点とし，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 $G=(V, E)$ で表す．各辺に対応する鍵は事前に何らかの方法で共有されており，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 $H \subseteq E$ がある確率分布に従って生起し，その漏えい辺集合 H に含まれる全ての鍵が盗聴されているとする．このようなグラフと確率分布の対を部分的漏えい鍵共有グラフと呼ぶ．この状況で2人のプレイヤーs, t が他のプレイヤーと協力して，s, t 間でできるだけ Eve に漏えいしていない1ビットの秘密鍵を共有したいという問題を考える．

2. 既知の結果と本稿の成果

前節で述べた問題を解決するプロトコルとして，st-フロープロトコルが知られており，これを用いると 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[1]．一方で，グラフの全ての辺(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．その解決のため，一様漏えい鍵共有完全グラフ(詳しくは次節)に対して，$l \leqq 2n-3$ を満たす ℓ 本(ただし l は奇数とする)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 $p(2p-p^2)^{\frac{l-1}{2}}$ と解析的に求まる[2]．

しかし，それ以外の場合について Eve への漏えい確率を解析的に求めることは未だ解決していないため，ユーザーにとって適切な鍵選択を行うことが困難である．本稿では，適切な鍵選択を行う為の基盤として，全ての鍵を用いた場合，即ち既存の st-フロープロトコルを用いた場合についての Eve への漏えい確率を解析的に求めるための漸化式を示し，二者鍵共有の限界を明確にする．

3. 漏えい確率を与える漸化式

本稿では，部分的漏えい鍵共有グラフとして，簡単の為，一様漏えい鍵共有完全グラフを仮定する．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 は完全グラフであると仮定する．

$(a+b+k)$ 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 $L(a, b; k)$ と書くことにすると，次の漸化式が得られる．

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

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

$k > 1$ の場合

$$\begin{aligned} &L(a, b; k) \\ &= p^{ab}\{p^{ak} + p^{bk} - p^{(a+b)k} \\ &+ \sum_{i=1}^{k-1} \sum_{j=1}^{k-i} {}_kC_{i\,k-i} C_j (1-p^a)^i p^{a(k-i)} (1 \\ &- p^b)^j p^{b(k-j)} L(i, j; k-i-j)\} \end{aligned}$$

式中の i は a 点クリークから漏えいしていない辺を通って k 点の内丁度 i 個に到達できることと対応し，j も同様である．

4. 漏えい確率の具体例

既存の st-フロープロトコルを用いた際の Eve への漏えい確率(下限)は，定義した漸化式をもとに，$L(1, 1; n-2)$ で与えられる．その値と，$l=2n-3$ を満たす鍵選択をした際の Eve への漏えい確率([2]の手法)を $p=0.75, 0.5, 0.25$ の場合について図1に例示する．

これにより，全ての鍵を使うべきか，$2n-3$ 本の鍵で十分かを判断する指標となることが期待される．

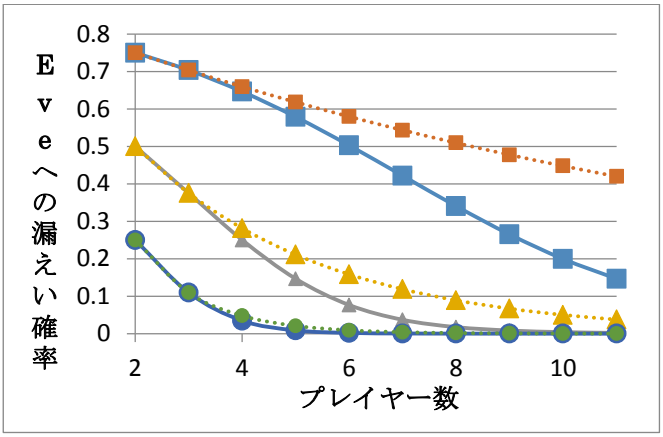

図1　Eve への漏えい確率
直線が下限，点線が[2]の手法．また■，▲，●はそれぞれ $p=0.75$，0.5，0.25 の場合を示す．

5. まとめ

st-フロープロトコルを用いる際に適切な鍵選択を行う為の基盤として，Eve への漏えい確率の下限を求める漸化式を示した．

今後の課題として，完全グラフ以外のグラフに一般化し，ユーザーが具体的に Eve への漏えい確率を得られる手法を考案することが挙げられる．

参考文献

[1] Takaaki Mizuki, et al. "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] 松田重裕他，"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.