C-028

大規模な RFID システムにおけるスキップグラフを用いた認証
A Study of Authentication Using a Skip Graph for Large-scale RFID Systems

小森 雄大 † 酒井 和哉 ‡ 福本 聡 ‡
Yudai KOMORI Kazuya SAKAI Satoshi FUKUMOTO

1. はじめに

RFID (Radio Frequency Identification) システムのプライバシーを守るために，暗号ベース認証を用いる方法がある．暗号ベース認証は，タグの数が膨大になると，認証に用いる鍵の検索に時間がかかる．そこで認証時間を改善するために，様々な鍵管理の構造化手法が研究されてきた．本研究では，鍵管理にスキップグラフを応用した認証プロトコルである RSGA(Randomized Skip-Graph Authentication) を提案する．そして，シミュレーションにより認証時間と匿名性が向上することを示し，大規模なシステムで運用可能であることを示す．

2. 暗号ベース認証

第三者がタグとリーダ間の通信を盗聴して入手したタグ ID を使用して，バックエンドサーバから情報を盗む攻撃がある．Weis が提案した Hash-lock[3] は，タグ ID の代わりにタグ ID とタグ固有の鍵から作られたハッシュ値を返信に用いる．Hash-lock では第三者に通信を盗聴された場合でも，タグの ID を特定されることは無い．しかし，認証に用いる鍵の検索に時間がかかるので，大規模なシステムには向いていない．そこで，鍵の管理に構造化を用いる方法が研究されている．

構造化手法によるプライベートタグ認証プロトコル [1, 2] は，タグ固有の鍵の他にグループ鍵と呼ばれる鍵を用いることで，鍵の検索範囲を狭めることができる．図 1 は，木構造ベースの鍵管理手法である．葉ノードにタグ固有の鍵 (sk)，非葉ノードにグループ鍵 (gk) を割り当てている．認証の際にタグ固有の鍵を検索する前に，グループ鍵を用いて検索範囲を狭めてからタグ固有の鍵を検索するので，検索時間は非構造化の場合よりも短くなる．

3. システムの匿名性

RFID システムにおけるプライバシーを守るためには，タグ ID を第三者に開示しない，タグの匿名性が確保されている必要がある．ここでは，システム のプライバシーの指標について説明する．

3.1 危惧化

Hash-lock のような暗号ベース認証でタグの応答を保護した場合，第三者は応答からタグ ID を盗むことが出来ない．しかし，タグのメモリを物理的に解析することで，タグ ID を盗むことは可能である．本研究では，タグに対する物理的な攻撃を危惧化と呼ぶ．危惧化は物理的な攻撃なので，危惧化自体を防ぐことは本研究の範囲外である．

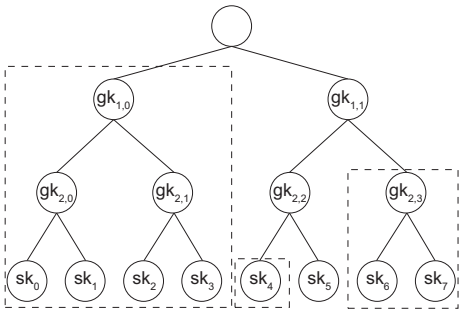

図 1: 木構造ベース

3.2 匿名集合

タグの匿名性の指標として匿名集合を考える．匿名集合はタグ ID を第三者に知られていないタグの集合である．危惧化などにより，第三者にタグ ID を知られた場合の匿名集合の大きさは 1 とする．匿名集合が大きいほど第三者にタグ ID を特定される確率が小さくなる．

システム内のタグの総数が $N = 8$ 個の場合，鍵管理に構造化を用いてない暗号ベース認証を用いると，全てのタグにおいて匿名集合の大きさは 8 になる．しかし，システム内のタグが $N_c = 4$ 個危惧化されると，危惧化されていないタグの匿名集合の大きさは 4 になり，危惧化されたタグの匿名集合の大きさは 1 になる．このように，鍵管理に構造化を用いてない場合におけるタグの匿名集合は，一つもタグが危惧化されていない場合は全て N，N_c 個のタグが危惧化された場合は $N - N_c$ もしくは 1 になる．

次にシステム内のタグの総数が $N = 8$ 個のとき，鍵管理に木構造を用いた場合を考える．図 1 のタグ固有の鍵 sk_5 を持つタグ 5 が危惧化されたとすると，悪意のある第三者はタグ 5 のグループ鍵を全て入手することになる．そして，他のタグの応答を盗聴し盗んだグループ鍵を使うことで，部分的に応答から情報を得ることが出来る．この場合，全く同じグループ鍵を使うタグ 4 の匿名集合は 1 に，$gk_{1,1}$ だけ共有するタグ 6, 7 の匿名集合は 2 に，一つも同じグループ鍵を共有しないタグ $0, 1, 2, 3$ の匿名集合は 4 になる．このように，鍵の管理に構造化を用いると，あるタグが危惧化されたときに他のタグの匿名集合の大きさが大幅に小さくなる．

†首都大学東京 大学院 システムデザイン研究科, Graduate School of System Design, Tokyo Metropolitan University
‡首都大学東京 システムデザイン学部, Faculty of System Design, Tokyo Metropolitan University

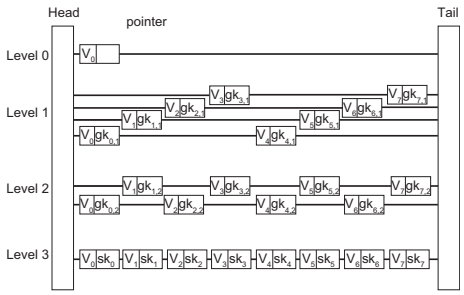

図 2: RSGA の構造

システムの匿名性は $A = \frac{1}{N^2}\sum_i |S_i|^2$ で求められる．ここで，S_i はタグ i の匿名集合である．システム内の各タグの匿名集合が大きい方がシステムの匿名性は大きくなる．

4. RSGA

RSGA は，図 2 に示すようなスキップグラフを用いたプライベート認証プロトコルである．スキップグラフはスキップリストの拡張で，異なる点はスキップリストが各階層に双方向リストが一つだけ存在するのに対し，スキップグラフでは各階層に複数の双方向リストが存在する点である．一番レベルが高い階層 (Level3) には全てのノードから作られた双方向リストが一つだけ存在し，それぞれタグが一つ割り振られている．それ以外の階層にはそれぞれ双方向リストが 2 つ以上存在し，各ノードにグループ鍵が割り振られている．Level0 は例外で，何も割り振られていないノードが一つだけ存在する．鍵の発行は各タグが各階層でランダムシフトをしながら，スキップグラフを探索することによって行う．

ここで，タグが持つグループ鍵の集合が他のタグと全く同じになる確率を考える．ここではその確率を相関確率と呼ぶ．RSGA とスキップリストベースの RSLA [2] は，各階層でランダムシフトをしているので，あるタグが危惧化されてもそのタグと全く同じグループ鍵を共有しているタグが存在しないかぎり，匿名集合は小さくならない．したがって，相関確率を小さくすることは，システムの匿名性を確保する上で重要になる．システムに存在するタグの総数を N，枝数を k とすると，RSLA の相関確率は $\Pi_{i=1}^{\lceil log_k N \rceil - 1} \frac{1}{k^i}$ となる．一方 RSGA の相関確率は，$\frac{1}{N}^{\lceil log_k N \rceil - 1}$ となる．RSGA の方が RSLA より各階層に存在するノードの数が多いため，相関確率は小さくなる．

5. シミュレーション結果

図 3 はタグの総数を 4096，枝数を k としたときの危惧化されたタグの割合に対するシステムの匿名性である．比較したプロトコルは木構造，AnonPri[1]，RSLA，RSGA である．RSLA と RSGA のシステムの匿名性は，既存のプロトコルよりも大幅に向上している．また，10%

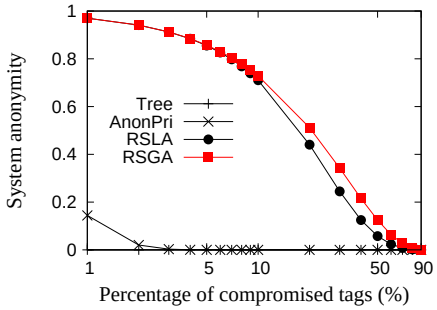

図 3: システムの匿名性

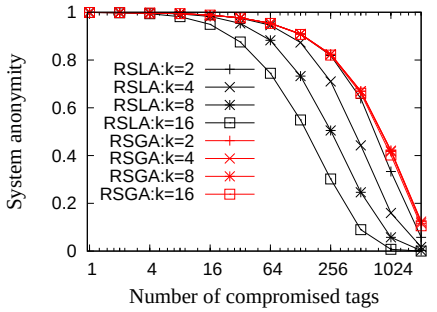

図 4: 枝数 k に対するシステムの匿名性

から 50% の危惧化率のとき，RSLA に比べて RSGA の方がシステムの匿名性が向上している．

図 4 は RSLA と RSGA の枝数 k を変えたときのシステムの匿名性である．RSLA は枝数が増えるとシステムの匿名性が減少しているが，RSGA は減少していない．システムに参加できるタグの数を増やす方法として，木の高さを増やす方法と枝数を増やす方法がある．木の高さを増やすとグループ鍵も増えるが，タグのメモリには制限があるので，増やせる木の高さには限界がある．したがって，大規模システムで運用するためには，枝数を増やす必要がある．RSLA とは違い RSGA は，枝数とシステムの匿名性に関係性が無いので，RSGA は大規模なシステムに適用できると言える．

6. まとめ

本論文ではスキップグラフを応用したプライベート認証プロトコルである RSGA を提案し，シミュレーションによって既存のプロトコルと性能を比較した．RSGA は各階層のノードを増やすことで，既存のプロトコルよりも高いシステムの匿名性を実現した．また，枝数を増やすことで大規模なシステムで運用することが出来る．

参考文献

[1] M. E. Hoque, F. Rahman, and S. I. Ahamed. AnonPri: An Efficient Anonymous Private Authentication Protocol. In *PerCom*, pages 102–110, 2011.

[2] M.-T. Sun, K. Sakai, W.-S. Ku, T. H. Lai, and A. V. Vasilakos. Private and Secure Tag Access for Large-Scale RFID Systems. *IEEE Trans. Dependable and Secur. Compt., in press.*

[3] S. A. Weis. Security and Privacy in Radio-Frequency Identification Devices. *Master Thesis, MIT*, 2003.