

A New Secret Key Agreement in a Four-Terminal Network



**Parisa Babaheidarian, Somayeh Salimi,
and Mohammad Reza Aref**

Information Systems and Security Lab (ISSL)

Department of Electrical Engineering,

Sharif University of Technology, Tehran, Iran





Outline

- Introduction
- Motivation
- Our contribution
- Main Results
 - The inner bound
 - Special Cases
- Discussion and summary
- References



Introduction

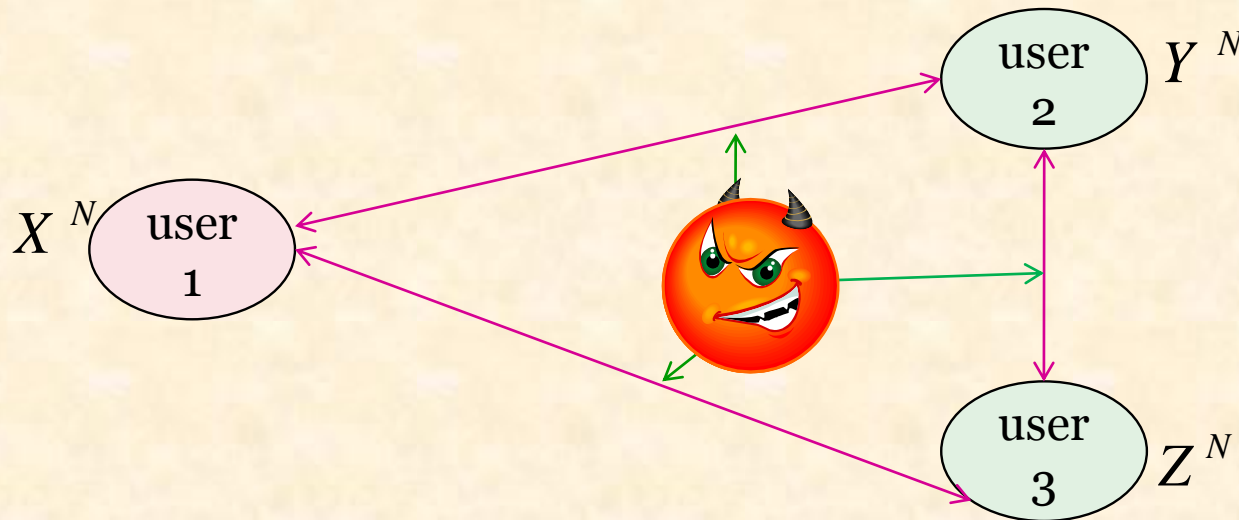
- The secret key agreement was first studied by Maurer in 1993. secret key agreement by public discussion based on common information. [1]
- Two concepts were studied
 - Utilizing a noiseless public channel
 - Having distinct correlated sources
- Problem of generating common randomness was then studied in the work of Ahlswede and Csiszár.[3]
 - Channel model and source model were introduced.
 - Forward capacity region was derived for both channel model and source model.
- Necessary and sufficient conditions for inner and outer bounds of the secret key capacity was studied in a valuable work by A. A. Gohari and V. Anantharam. [4]



Motivation

4

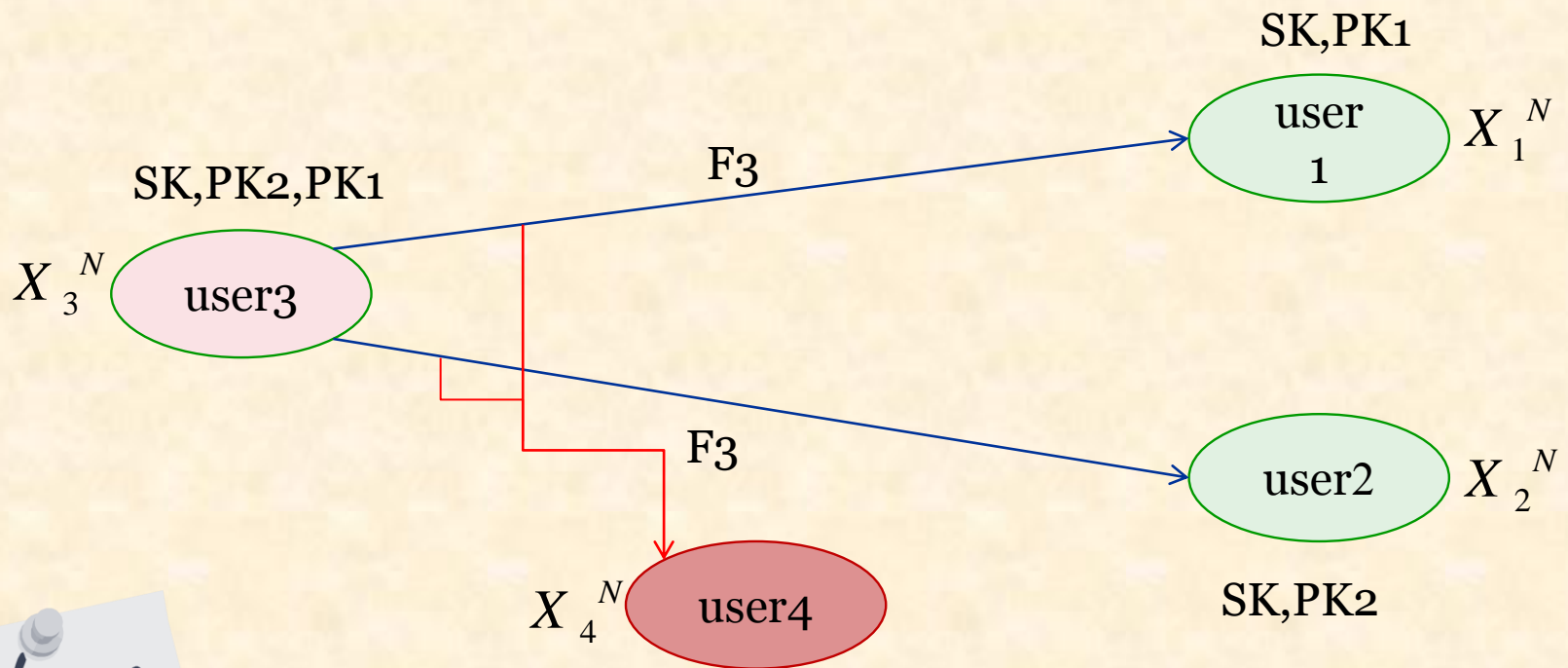
- Generating multiple keys in a group of terminals.
 - Sharing the secret key and private keys among terminals.
 - First studied in a work by C. Ye and P. Narayan, The Secret key-Private key Capacity Region for Three Terminals.(2004-2005)





Our Contribution

5





Achievable Region

$$R^I = \text{Conv} \bigcup_{P(u_0, u_1, u_2, x_1, x_2, x_3, x_4, q)}$$

$$\left\{ \begin{array}{l} (R_0, R_1, R_2): \\ R_0 \geq 0, R_1 \geq 0, R_2 \geq 0 \\ R_0 \leq [\min\{I(U_0; X_1 | Q), I(U_0; X_2 | Q)\} - I(U_0; X_4 | Q)]^+ \\ R_1 \leq [I(U_1; X_1 | U_0, Q) - \\ \max\{I(U_1; X_2, U_2 | U_0, Q), I(U_1; X_4, U_2 | U_0, Q)\}]^+ \\ R_2 \leq [I(U_2; X_2 | U_0, Q) - \\ \max\{I(U_2; X_1, U_1 | U_0, Q), I(U_2; X_4, U_1 | U_0, Q)\}]^+ \end{array} \right.$$

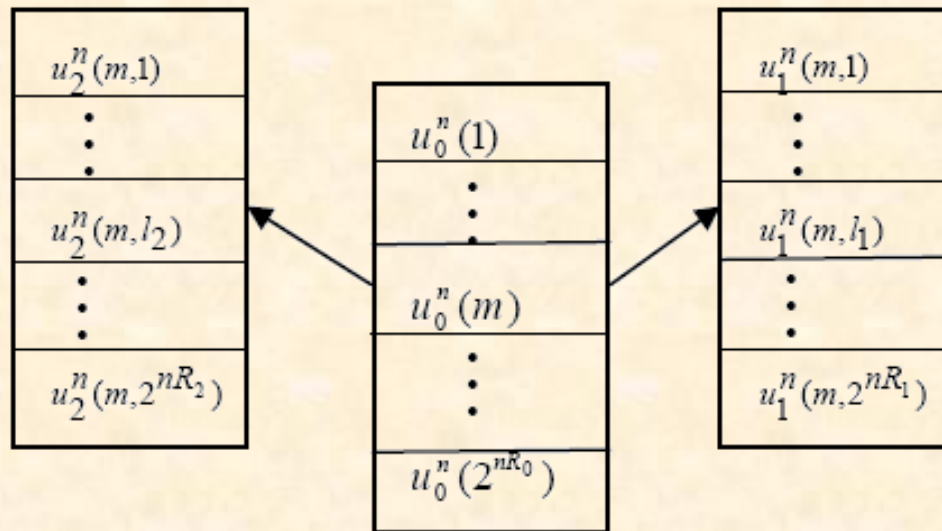
$$p(u_0, u_1, u_2, x_1, x_2, x_3, x_4, q) = p(q | u_0, u_1, u_2) p(u_0 | x_3) p(u_1 | u_0, x_3) p(u_2 | u_0, x_3) \\ p(x_1, x_2, x_3, x_4)$$



The Coding Scheme

7

- Coding scheme
 - Double-layer random binning
 - Superposition coding (Secret Superposition scheme [8])





Explicit upper bound

8

- **Proposition 1:** In the key agreement scenario of the described model, if the rate triple is achievable, then it satisfy:

$$\left\{ \begin{array}{l} R_0 \leq \min \{I(X_3; X_1 | X_4), I(X_3; X_2 | X_4)\} \\ R_1 \leq \min \{I(X_3; X_1 | X_4), I(X_3; X_1 | X_2)\} \\ R_2 \leq \min \{I(X_3; X_2 | X_4), I(X_3; X_2 | X_1)\} \end{array} \right\}$$



Special cases (Markov chains)

9

- When the source observations form a Markov chain as $X_3 - X_1 - X_4 - X_2$ the secret key-private keys capacity region reduces to:

$$R_0 = 0, R_2 = 0, 0 \leq R_1 \leq I(X_3; X_1 | X_4)$$

- When the source observations form a Markov chain as $X_3 - X_1 - X_2 - X_4$ the secret key-private keys capacity region reduces to:

$$0 \leq R_0 \leq I(U_0; X_2 | Q) - I(U_0; X_4 | Q),$$
$$0 \leq R_1 \leq I(U_1; X_1 | U_0, Q) - I(U_1; X_2 | U_0, Q), R_2 = 0$$



- When the source observations form a Markov chain as $X_2 - X_3 - X_1 - X_4$ the secret key-private keys capacity region reduces to:

$$0 \leq R_0 \leq I(U_0; X_2 | Q) - I(U_0; X_4 | Q),$$

$$0 \leq R_1 \leq I(U_1; X_1 | U_0, Q) - I(U_1; X_2 | U_0, Q),$$

$$0 \leq R_2 \leq I(U_2; X_2 | U_0, Q) - I(U_2; X_1 | U_0, Q)$$

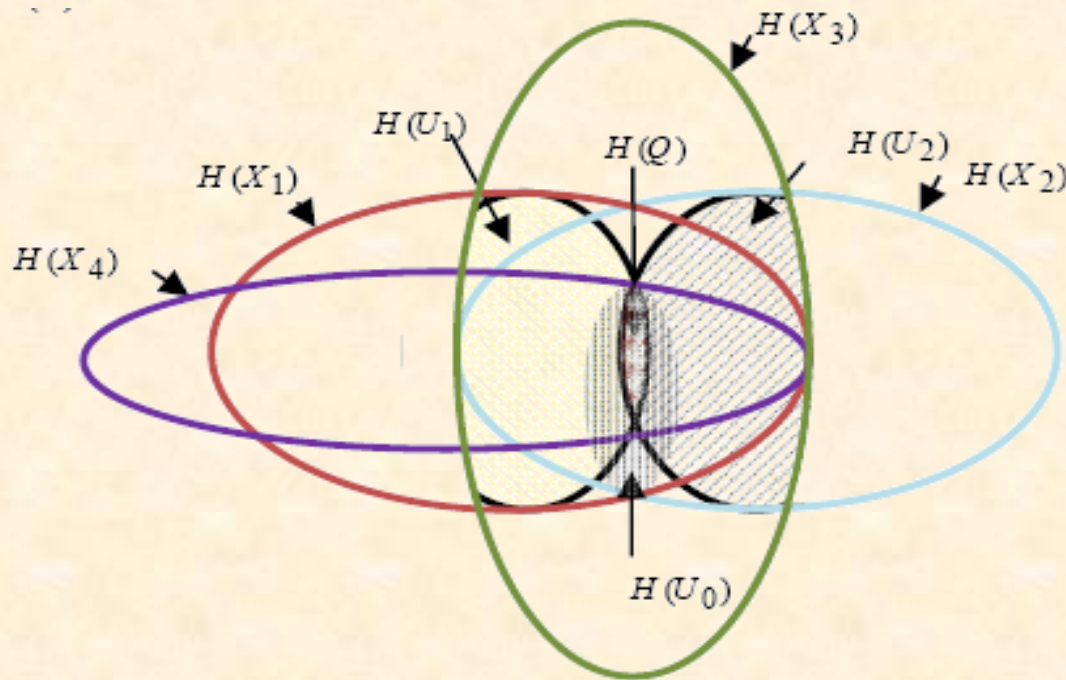
For all auxiliary random variables which satisfy:

$$U_0 - (Q, X_1) - (Q, X_2) \quad U_1 - (U_0, Q, X_1) - (U_0, Q, X_2) - U_2 \quad U_2 - (U_1, U_0, Q, X_2) - (U_1, U_0, Q, X_4)$$



An example

- This situation is illustrated in the figure below:



An example for case $X_2 - X_3 - X_1 - X_4$



Summary and Discussion

- Studying a new source model of secret key sharing
- Inner bound for Secret key-Private keys capacity region is derived.
- Special cases were found that inner bound is the keys capacity.(tightness)
- As a continue of this works we have also studied the reverse case.(Forward Strategy)
- One can study the case of having three private keys
- Also we can have a helper node in a problem setup.



References

1. U. M. Maurer, “Secret key agreement by public discussion from common information,” *IEEE Trans. Inform. Theory*, vol. 39, 1993, pp. 733-742.
2. I. Csiszár and P. Narayan, “Common randomness and secret key generation with a helper,” *Information Theory, IEEE Transactions on*, vol. 46, 2002, pp. 344–366.
3. R. Ahlswede and I. Csiszár, “Common randomness in information theory and cryptography. i. secret sharing,” *Information Theory, IEEE Transactions on*, vol. 39, 2002, pp. 1121–1132.
4. A.A. Gohari and V. Anantharam, “Information-Theoretic Key Agreement of Multiple Terminals—Part I,” *Information Theory, IEEE Transactions on*, vol. 56, 2010, pp. 3973–3996.
5. C. Ye and P. Narayan, “The private key capacity region for three terminals,” *Information Theory, 2004. ISIT 2004. Proceedings. International Symposium on*, 2005, p. 44.



6. C. Ye and P. Narayan, “The secret key\ private key capacity region for three terminals,” *Information Theory, 2005. ISIT 2005. Proceedings. International Symposium on*, 2005, pp. 2142–2146.
7. S. Salimi, M. Salmasizadeh, and M.R. Aref, “Secret key sharing in a new source model: Rate regions,” *Communications Theory Workshop (AusCTW), 2010 Australian*, 2010, pp. 117–122.
8. G. Bagherikaram and A. S. Motahari and A. K. Khandani, “The secrecy rate region of the broadcast channel,” in *Proceedings of the Allerton Conference on Communications, Control and Computing*, July 2008.
9. I. Csiszár and P. Narayan, “Secrecy capacities for multiple terminals,” *Information Theory, IEEE Transactions on*, vol. 50, 2004, pp. 3047–3061.
10. A. D. Wyner, “The wire-tap channel,” *Bell Sys. Tech. J.*, vol. 54, 1975, pp.1355-1387.



The End