如何产生和交换秘密

姚期智, 普林斯顿大学计算机科学系

翻译：李晓峰 (cy_lxf@163.com)*

V1.0

2024 年 6 月 25 日

摘要

本文介绍了一种控制密码协议设计中知识传递过程的新工具。它被应用于解决一类一般的问题，其中包括文献中大多数的两方密码问题。具体来说，我们展示了双方 A 和 B 如何交互地生成一个随机整数 $N = pq$，使得其秘密，即质因数 (p, q)，对任何一方都是单独隐藏的，但如果需要，可以共同恢复。利用该模型，可以给出一个协议，使具有私有值 i 和 j 的双方在具有最小知识转移和强公平性 (strong fairness property) 的前提下，计算任意多项式可计算函数 $f(i, j)$ 和 $g(i, j)$。作为一个特例，A 和 B 可以交换一对秘密 S_A, S_B，例如分解一个整数和图中的一个哈密顿回路，使得当且仅当 S_B 能被 A 计算时，S_A 也能被 B 计算。所有这些结果都是在假定大数分解问题是计算困难的情况下证明的。

*译文来自于经典文献翻译项目 https://gitee.com/uisu/InfSecClaT, 欢迎大家加入经典翻译项目，为更多的人能够获取这些经典文献所传递信息做一点贡献。

I 引言

II 术语

III 生成一个秘密

IV 交换一个秘密

V 通用计算

VI 正确性

参考文献

[ACGS] W . Alexi , B . Chor , O . Goldreich , and C . P . Schnorr , ” RSA / Rabin bits are l / 2 - f l / 2 poly (log n) secure , ” Proceedings of 25 th Annual IEEE Symposium on Foundations of Computer Science , 1984 , 449 - 457 .

[Bl] M . Blum , ” Coin flipping by phone , ” COMPCON (1982) ,133 - 137 .

[B 2] M . Blum , ” How to exchange (secret) keys , ” ACM Transactions on Computer Systems 1 (1983) , 175 - 193 .

[BS] M . Blum and S . Goldwasser , ” An efficient probabilistic PKCS as secure as factoring , ” Proceedings of Crypto 84 , 1984

[C] R . Cleve , ” Limits on the security of coin flips when half of the processors are faulty , ” Proceedings of 18 th Annual ACM Symposium on Theory of Computing , 1986 , 364 - 369 .

[FMRW] M . Fischer , S . Micali , C . Rackoff , and D . Wittenberg , ” An oblivious transfer protocol , ” 1985 , to appear .

[GHY] Z . Galil , S . Haber , and M . Yung , ”A private interactive test of a Boolean predicate and minimum - knowledge public - key cryptosystems , ” Proceedings of 26 th Annual IEEE Symposium on Foundations of Computer Science , 1985 , 360 - 371 .

[GM] S . Goldwasser and S . Micali , " Probabilistic encryption and how to play mental piker keeping secret all partial information , " Proceedings of 14 th Annual ACM Symposium on Theory of Computing , 1982 , 365 - 377 .

[GMR] S . Goldwasser , S . Micali , and C . Rackoff , " The knowledge complexity of interactive proof systems , " Proceedings of 17 th Annual ACM Symposium on Theory of Computing , 1985 , 291 - 304 .

[GMW] 0 . Goldreich , S . Micali , and A . Wigderson , " Proofs that yield nothing but their validity and a methodology of cryptographic protocol design , " Proceedings of 27 th Annual IEEE Symposium on Foundations of Computer Science , 1986

[HS] J . Hastad and A . Shamir , " The cryptographic security of truncated linearly related variables , " Proceedings of 17th Annual ACM Symposium on Theory of Computing , 1985 , 356 - 362 .

[LMR] M . Luby , S . Micali , and C . Rackoff , " How to simultaneously exchange a secret bit by flipping a symmetrically based coin , " Proceedings of 24 th Annual IEEE Symposium on Foundations of Computer Science , 1985 , 11 - 22 .

[R] M . Rabin , " How to exchange secrets , " 1981 , unpublished manuscript .

[SRA] A . Shamir , R . Rivest , and L . Adleman , " Mental Poker , " MIT Technical Report , 1978

[T] T . Tedrick , " How to exchange half a bit , " Crypto ' 88 .

[VV] U . Vazirani and V . 'Vazirani , " Trapdoor pseudo - random number generators , with applications to protocol design , " Proceedings of 24 th Annual IEEE Symposium on Foundations of Computer Science , 1985 , 23 - 30 .

[Yl] A . Yao , " Protocols for secure computations , " (extended abstract) Proceedings of 21 st Annual IEEE Symposium Foundations of Computer Science , 1982 .

[Y 2] A . Yao , " Protocols for secure computations , " in preparation .

[Y 3] A . Yao , " Theory and applications of trapdoor functions

, ” Proceedings of 21 st Annual IEEE Symposium on Founda - tions of Computer Science , 1982