The Fabbrini Problem

Ed Andersen

Eindhoven University of Technology
Orcid: https://orcid.org/0009-0005-5789-5209

June 20, 2023

Abstract

This document intends to emphasize some aspects of a recent algorithm capable of generating a secret key by transmitting information over a public channel. Given that the scheme's construction is engaging and represents a topical innovation, we deem it useful to refer to it as "The Fabbrini Problem", after its author.

Keywords— *circular multiplicative modular exponentiation, public key cryptography*

1 The Fabbrini Problem

The Circular Multiplicative Modular Exponentiation algorithm (CMME) is a new public key exchange algorithm that was proposed by Michele Fabbrini in 2023 [1]. It is based on the idea of circular multiplicative modular exponentiation, which means that two parties can generate a shared secret key by multiplying the modular exponentiation of two bases and their private exponents, and then exchanging the results over a public channel. The algorithm is claimed to be more secure than the traditional Diffie-Hellman scheme. Using two bases and two exponents as an example, the Fabbrini Problem (FP) can be stated as follows.

Given

- a prime p
- two of its primitive roots, (g_1, g_2)
- four random integers less than p, (a_1, a_2, b_1, b_2)
- four more integers $(A_1 = g_1^{a_1} g_2^{a_2}, A_2 = g_1^{a_2} g_2^{a_1}, B_1 = g_1^{b_1} g_2^{b_2}, B_2 = g_1^{b_2} g_2^{b_1})$

Find one of the following sets

- $KA_1 = B_1^{a_1} B_2^{a_2}, KA_2 = B_1^{a_2} B_2^{a_1}$
- $KB_1 = A_1^{b_1} A_2^{b_2}, KB_2 = A_1^{b_2} A_2^{b_1}$
- $KA_1 = B_1^{a_1} B_2^{a_2}, KB_2 = A_1^{b_2} A_2^{b_1}$
- $KB_1 = A_1^{b_1} A_2^{b_2}, KA_2 = B_1^{a_2} B_2^{a_1}$

2 Security against the "Small Subgroup Attack (SSA)"

In our opinion, CMME is more secure than Diffie-Hellman, because it is resistant to small subgroup attacks [2] [3] [4], which exploit the structure of the underlying group. CMME resists small subgroup attacks by using a circular multiplicative modular exponentiation function that prevents an attacker from forcing a key to be confined to a small subgroup of the desired group. A small subgroup attack is a type of attack on a key exchange protocol that uses a large finite group, such as Diffie-Hellman, where an attacker tries to compromise the protocol by making a key belong to a small subgroup of the group, which makes the exhaustive search for the key feasible in practice. CMME avoids this problem by using multiple bases and exponents.

References

[1] Fabbrini, Michele "Circular Multiplicative Modular Exponentiation: A New Public Key Exchange Algorithm." Cryptology ePrint Archive (2023)

[2] Law, Laurie, et al. "An efficient protocol for authenticated key agreement." Designs, Codes and Cryptography 28 (2003): 119-134.

[3] Lim, Chae Hoon, and Pil Joong Lee. "A key recovery attack on discrete log-based schemes using a prime order subgroup." Advances in Cryptology—CRYPTO'97: 17th Annual International Cryptology Conference Santa Barbara, California, USA August 17–21, 1997 Proceedings 17. Springer Berlin Heidelberg, 1997.

[4] Ferguson, Niels, and Bruce Schneier. Practical cryptography. Vol. 141. New York: Wiley, 2003.