PHYS.ORG

The complexity and security of a widely-used cryptography scheme are lower than previously thought

May 18 2016

The equations used to construct a digital security scheme based on the 'hidden field equation' (HFE) theory can be solved much more easily than originally believed, an A*STAR-led mathematical and computational study has shown.

HFE is a computer cryptography scheme that uses a set of polynomial equations to generate encrypted values that only the holder of a private key can decrypt. The security of the scheme is based on the difficulty of solving these specially designed, multifactor polynomial systems.

"HFE was introduced over 20 years ago, and since then there have been several experimental studies that have suggested that the polynomial systems underlying the HFE cryptosystems seem to be much easier to solve compared to, say, random systems," says Sze Ling Yeo from the A*STAR Institute for Infocomm Research. "For instance, the HFE encryption was successfully broken in 2003 in just 96 hours. In our work, we give the first theoretical proof explaining why the polynomial systems in the HFE scheme are easier to solve."

The polynomials used to construct the HFE scheme each typically involve hundreds of variables that describe complex curves, and cracking such systems requires all of the variables of the polynomial to be found. Theoretically such a scheme offers a very high level of security, but because the scheme involves other parameters that describe the special design of the set of polynomials, there are mathematical shortcuts to solving them.

It was previously thought that as the number of terms in the polynomial equation used to construct the HFE system increased, the complexity of the solution—the number of equations that need to be generated to solve the problem—would increase exponentially, making decryption almost impossible in realistic timeframes even using next-generation computational technology. However, Yeo in collaboration with Ming-Deh Huang from the University of Southern California and Michiel Kosters from Nanyang Technological University were able to show that because the HFE system is not composed of random polynomials, but instead uses rules for their construction, it can be solved by common mathematical methods without exponential complexity.

"Polynomial systems such as these arise in other cryptographic problems too, including techniques to solve one of the better modern cryptography schemes called the elliptic curve discrete logarithm problem, or ECDLP," says Yeo. "So, understanding the complexity of solving these polynomial systems is important beyond merely breaking the HFE cryptosystems. Our work highlights the importance of being more rigorous in proving complexity claims."

More information: Huang, M.-E. A., Kosters, M., Yeo, S. L. (2015) Last fall degree, HFE, and Weil descent attacks on ECDLP. In R. Gennaro & M. Robshaw (Eds.) *Advances in Cryptology*—CRYPTO 2015. DOI: 10.1007/978-3-662-47989-6_28

Provided by Agency for Science, Technology and Research (A*STAR), Singapore

Citation: The complexity and security of a widely-used cryptography scheme are lower than previously thought (2016, May 18) retrieved 10 April 2024 from https://phys.org/news/2016-05-complexity-widely-used-cryptography-scheme-previously.html