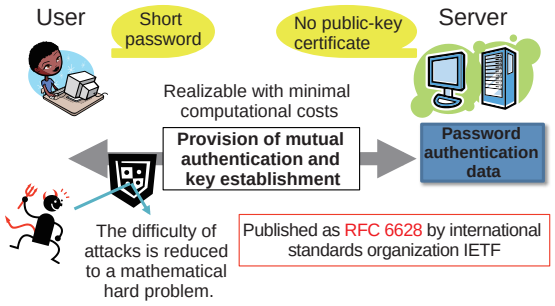
Authentication scheme secure against eavesdropping and phishing attacks

Efficient and provably secure password-based authentication scheme

We have developed a provably secure password-based authentication scheme which requires less computation costs than those of the previous schemes. This authentication scheme was adopted as a standard of efficient password-based authentication schemes by the international standards organization IETF (Internet Engineering Task Force), and it was published as experimental RFC (Request for Comment) 6628 in June 2012. This authentication scheme is secure against various attacks including eavesdropping/modification/replay of communications, man-in-the-middle attacks, phishing scams, and server compromise impersonation attacks. In addition, its security is proven to be equivalent to a mathematical hard problem, meaning that it is almost impossible to break this scheme. Also, this authentication scheme provides high usability because users do not need to use long passwords and any complex public-key management system, i.e. key generation/confirmation/revocation procedures. Since it was published as an international standard, it is expected that this authentication scheme would be plugged into diverse internet services and applications in the near future.

SeongHan SHIN
seonghan.shin@aist.go.jp
Kazukuni KOBARA
k-kobara@aist.go.jp
Research Institute for Secure Systems
AIST TODAY Vol.13 No.2 p.12 (2013)



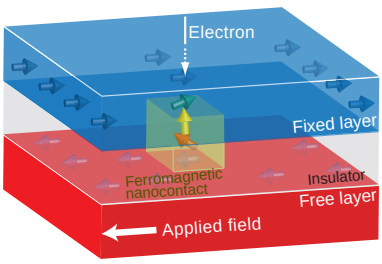
Features of the developed password-based authentication scheme

Millimeter-wave oscillation by ferromagnetic nanocontact device

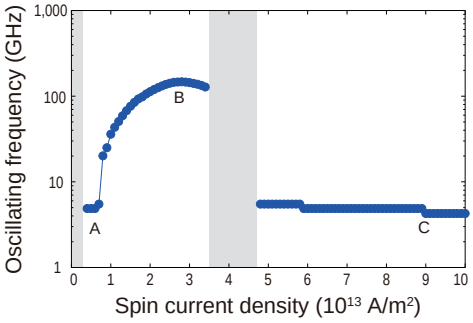
A theoretical proposal for a nanoscale current control-type oscillation device

Conventional giant magnetoresistive devices or ferromagnetic tunnel junction devices provide only low frequency oscillation and have been deemed unsuitable for applications requiring millimeter-wave (30–300 GHz) oscillation, including radar. However, upon analyzing precessional motion of spin induced by supplying a current to a ferromagnetic nanocontact device using a simulator developed by AIST, it was predicted that varying the current supplied to the ferromagnetic nanocontact device would cause the device to act as a current control-type oscillation device in the microwave to millimeter-wave range. If such a ferromagnetic nanocontact device is realized, it is expected to have applications in the next-generation wireless communication technology and sensor technology.

Hiroshi IMAMURA
Spintronics Research Center
h-imamura@aist.go.jp
AIST TODAY Vol.13 No.2 p.13 (2013)



Schematic diagram of ferromagnetic nanocontact and ferromagnetic electrode
The magnetic wall can be enclosed in the ferromagnetic nanocontact.



Current density dependence of oscillating frequency
Oscillations can be categorized into three characteristic regions, A, B, and C. The gray area indicates a region with no oscillation.