Young, nearby supernova remnant shows up

When supernova RXJ0852.0-4622 made its debut, the plague had not yet decimated Europe, Mongolians still ruled China, and two different dynasties vied for control of Japan. Appearing low in the sky across central Europe and Asia, the stellar explosion may have shone as brightly as Venus and could have been visible for a month.

No one knows for sure, since astronomers have no eyewitness account of this celestial event. But two teams of researchers, who have now discovered the remnant of this previously unknown explosion, say it's the closest supernova to have graced terrestrial skies during the past 1,500 years. Indeed, evidence suggests that the remnant resides a mere 600 light-years from Earth and that the stellar explosion from which it arose appeared in the southern sky only about 700 years ago.

Bernd Aschenbach of the Max Planck Institute for Extraterrestrial Physics in Garching, Germany, discovered the remnant while examining X-ray images taken by the satellite ROSAT. Aschenbach had set out to analyze the most energetic emissions from an elderly supernova remnant called Vela, but when he viewed images recorded at energies greater than 1,300 electron-volts, he found a faint object adjacent to Vela and with a similar circular form.

That shape is a hallmark of the shell of gas and dust ejected into space by a supernova. This newly found remnant shows up only at high energies because it is young and has not yet had enough time to cool, Aschenbach says.

Estimates of the remnant's temperature and its size in the sky suggest that it is no older than 1,500 years and no farther than 1,300 light-years from Earth, he reports in the Nov. 12 NATURE. "RXJ0852.0-4622 is likely to be the nearest supernova remnant in mankind's recent history."

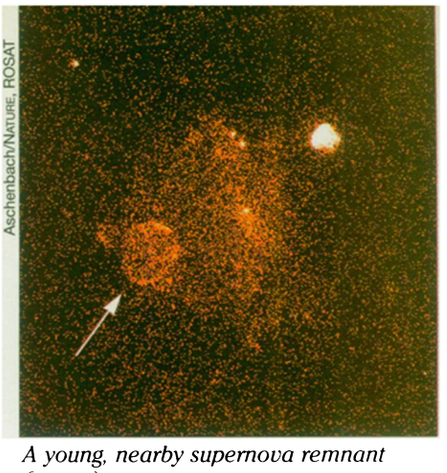
In the same issue of NATURE, Anatoli F. Iyudin, also of the Max Planck Institute and his colleagues, combine Aschenbach's observations with other measurements to place tighter limits on the remnant's distance and the time of the explosion. Iyudin used NASA's Compton Gamma Ray Observatory to search for gamma-rays emitted by titanium-44, a metal forged in supernovas and that has a half-life of only 90 years.

The team found emissions from titanium-44 in the same celestial region where Aschenbach had discovered the remnant. Using standard assumptions about the initial supply of the isotope, Iyudin and his colleagues estimate that the explosion occurred about 700 years ago.

"I doubt if I [would be] convinced by just one set of data, but the two combined make it a compelling case," says Robert Petre of NASA's Goddard Space Flight Center in Greenbelt, Md. "Titanium-44 is the clincher."

Robert P. Kirshner of the Harvard-Smithsonian Center for Astrophysics in Cambridge, Mass., notes that discovering young remnants is important because they retain details of the titanic explosions that produced them. Moreover, finding a young remnant in our own galaxy, he notes, helps fill a gap. Although astronomers calculate that a supernova goes off about once a century in the Milky Way, the last one seen was in 1604.

The lack of eyewitness accounts does not contradict the findings, says Bradley E. Schaefer of Yale University. Whether someone had written down the observation and whether such an account survived over several centuries remain as uncertain as the exact time of the explosion, he notes. Dust or gas along the line of sight to the supernova, as well as cloudy weather, could have dimmed the fireworks, Schaefer adds.



A young, nearby supernova remnant (arrow).

Researchers plan to search for radio signals from the remnant indicating whether the explosion left behind a cinder—a rapidly rotating neutron star. —*R. Cowen*

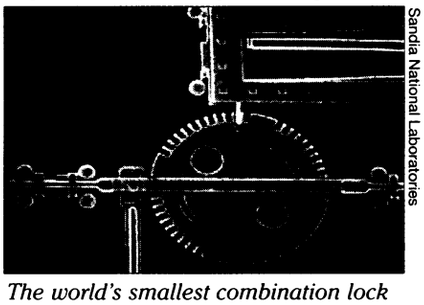
Lock-on-a-chip may close hackers out

Engineers have crammed an electromechanical combination lock onto a computer chip that they say can shut out cybercrooks. The device erects a barrier to computer intrusions that is far more difficult to penetrate than security software, the only option available today, say the lock's inventors.

Because security software does not physically isolate a system but monitors electronic codes, determined hackers on the Internet or a modem connection can keep trying passwords and other keys until they breach the defenses.

The new lock, however, accepts only one number among a million possibilities as its correct combination. If a remote troublemaker attempts a break-in with the wrong code just once, the device disconnects the computer from its network. When the lock closes, only someone physically present at the computer can reopen it.

The new lock, which employs concepts developed for protecting nuclear weapons, "puts a physical barrier between an asset and a threat," says the devices designer, Frank J. Peter of Sandia National Laboratories in Albuquerque, N.M. "And it absolutely, positively can't be circumvented in software."



The world's smallest combination lock uses this gear and five others, each about the size of the period at the end of this sentence, to mechanically test whether a would-be user has typed the correct computer-access number.

Peter and his colleagues have packed intricate machinery into the silicon device the size of a shirt button. Electrically driven shafts studded with microscopic teeth turn tiny gears to set the combination. If triggered by a bogus code, the mechanism throws a switch that interrupts the flow of electric current or light through the device, temporarily isolating the computer.

Such a drastic response may prove impractical except for restricted-use computer systems where a small number of users all know the code and someone is continuously on duty to reset machines, says Peter Mell of the National Institute of Standards and Technology in Gaithersburg, Md. Moreover, attackers can send trouble-causing electronic mail and other data without having to gain access to a computer by logging on. Hackers could also maliciously trigger the lock to deny use of computers to their owners, he notes.

During the next 2 years, the inventors may consider such questions in preparation for commercializing the technology. Perhaps they will choose to allow more than one false start, for instance, since computer users who rely on remote log-ins may occasionally type the wrong password. They also hope to find a company to mass-produce the locks inexpensively via methods used by integrated-circuit makers. —*P. Weiss*