Electronic Hotel Card Locks

These are wonderful little microcomputer projects masquerading as door locks.
Inside there's a processor running a program, with I/O
leads going to things like the magnetic strip reader, or the infrared LEDs, and
the solenoid, and the lights on the outside. They are
powered entirely by a battery pack, and the circuitry is designed such that it
draws almost nil power while idle. The cards are usually
magnetic-strip or infrared. The former uses an oxide strip like a bank card,
while the infrared card has a lot of holes punched in it. Since
IR light passes through most kinds of paper, there is usually a thin layer of
aluminum inside these cards. The nice thing about these
systems is that the cards are generally expendable; the guest doesn't have to
return them or worry about lost-key charges, the hotel can
make them in quantity on the fly, and the combination changes for each new guest
in a given room. The hotel therefore doesn't need a
fulltime key shop, just a large supply of blank cards. Duplication isn't a
problem either since the keys are invalidated so quickly.

The controlling program basically reads your card, validates the number it
contains against some memory, and optionally pulls a
solenoid inside the lock mechanism allowing you to enter. The neat thing about
them is that card changes are done automatically and
unknowingly by the new incoming guest. The processor generates new card numbers
using a pseudorandom sequence, so it is able to
know the current valid combination, and the *next* one. A newly registered guest
is given the *new* card, and when the lock sees that
card instead of the current [i.e. old guest's] card, it chucks the current
combination, moves the next one into the current one, and
generates the new next. In addition there is a housekeeping combination that is
common to all the locks on what's usually a floor, or
other management-defined unit.

There is no wire or radio connection to the hotel desk. The desk and the lock
are kept in sync by the assumption that the lock won't
ever see the "next" card until a new guest shows up. However if you go to the
desk and claim to have lost your card, the new one they
give you is often the "next" card instead. If you never use it and continue
using your old card, the guest after you will have the wrong
"next". In cases like this when the hotel's computer and the lock get out of
sync, the management has to go up and reset the lock. This
is probably done with a magic card that the lock always knows about [like in
ROM], and tells it something akin to "use this next card I'm
going to insert as the current combination". The pseudorandom sequence simply
resumes from there and everything's fixed. If the lock
loses power for some reason, its current memory will be lost but the magic
"reset" card will work.

Rumor has it that these locks always have a back-door means of defeating them,
in case the logic fails. Needless to say, a given
manufacturer's method is highly proprietary information. In theory the security
of these things is very high against a "random guess"
card since there are usually many bits involved in the combination, and of
course there is no mechanical lock to be manipulated or
picked. The robustness of the locking hardware itself sometimes leaves something
to be desired, but of course a lock designed for a hotel
door probably isn't the kind of thing you'd mount on your house.