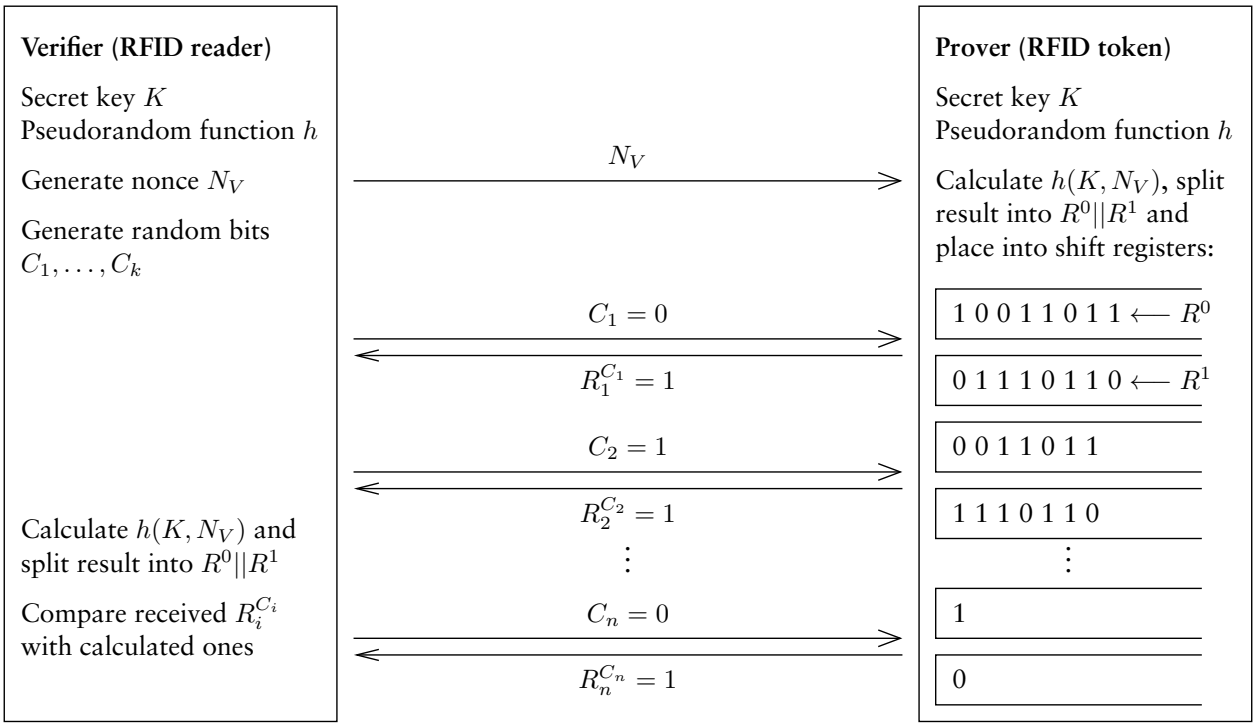
An RFID distance bounding protocol

UNIVERSITY OF CAMBRIDGE
Computer Laboratory
Security Group / TAMPER Lab

Gerhard P. Hancke, Markus G. Kuhn

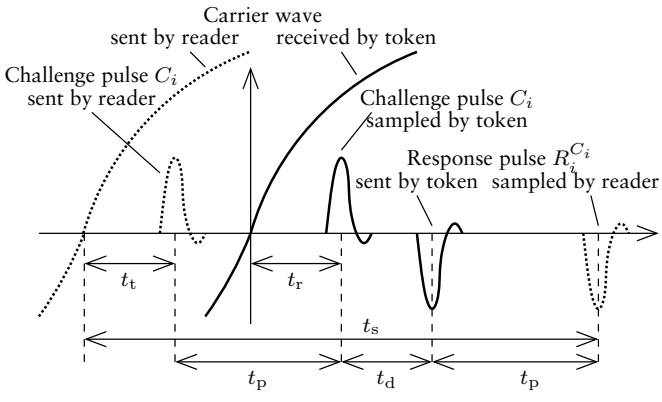
Authentication protocols estabish the identity of communication partners, by verifying their knowledge of a secret. Distance-bounding protocols establish, in addition, that the communication partner holding that secret is located within a given radius, assuming that information cannot propagate faster than at the speed of light. To verify small distances (in the order of meters or decimeters) special physical-layer arrangements have to be made for rapid single-bit roundtrip exchanges. We present a new such protocol, along with an outline implementation particularly suited for RFID applications. Our protocol tolerates bit errors in the rapid exchange phase, crucial for ultra-wideband pulse channels. The need for a stable frequency source or an accurate pulse-delay element is limited to the "verifier" (RFID reader), helping the implementation of the "proofer" (RFID token) meeting tight constraints (size, cost, power, manufacturing tolerances, no calibration).



$\langle C_i \rangle = 01001100$ will return $\langle R_i^{C_i} \rangle = 11010111$

Data layer: The challenge-response scheme used in the presented distance-bounding protocol consists of two phases. The first phase is not time-critical and calculates (typically in software) a response R to a challenge N_V, using a pseudorandom function h and a shared secret key S known to both parties. The $2n$ bits of R are not returned directly. Instead, they are split up and loaded into two n-bit shift registers. A preagreed fixed number of clock cycles after the transmission of N_V, the time-critical second phase begins, in which additional single-bit challenges C_i are transmitted. Each selects one of the two shift registers, which returns its first bit directly, using fast asynchronous logic that does not wait on any clock cycle. The first bit in the respective other shift register is discarded at the same time. This way, only half of all response bits R that were generated for an N_V are revealed.

Physical layer: The power-supply carrier wave emitted by the reader establishes a common time base for synchronizing the pulse communication of both parties. The token samples its wideband input at time t_r after a zero crossing of the carrier wave, to read a challenge bit C_i, and the reader must adjust its transmission delay $t_\mathrm{t} \approx t_\mathrm{r}$ such that its pulse arrives exactly at that time. The token responds with $R_i^{C_i}$ after a short, nearly constant switching delay t_d. The reader must adjust delay t_s until it receives the correct response, and can then deduce the upper distance bound $d = c \cdot (t_\mathrm{s} - t_\mathrm{t} - t_\mathrm{d})/2$.



G.P. Hancke, M.G. Kuhn: *An RFID distance bounding protocol.* Proceedings IEEE SecureComm 2005, ISBN 0-7695-2369-2.
`http://www.cl.cam.ac.uk/~mgk25/sc2005-distance.pdf`