

More hidden bits

D. J. Bernstein

University of Illinois at Chicago

Secret matrix $M \in \mathbf{F}_2^{100 \times 200}$.

Reader sends $d \in \mathbf{F}_2^{100}$.

Tag generates $e \in \mathbf{F}_2^{100}$,
sends $M(d, e) \in \mathbf{F}_2^{100}$.

Tag also sends e
with 20 erasures.

Reader searches all 2^{20}
possibilities for erased bits.

This “hidden bits” protocol is
RFIDsec 2012 Klonowski–
Majcher–Macyna–Zagórski.

This “hidden bits” protocol is
RFIDsec 2012 Klonowski–
Majcher–Macyna–Zagórski.

Secure? I’m skeptical.

But maybe erasing more bits
will improve security.

This “hidden bits” protocol is
RFIDsec 2012 Klonowski–
Majcher–Macyna–Zagórski.

Secure? I’m skeptical.

But maybe erasing more bits
will improve security.

Improved reader algorithm:
recompute e from $M(d, e)$
by linear algebra.

Insist on $M(0, \cdot)$ invertibility.

This “hidden bits” protocol is
RFIDsec 2012 Klonowski–
Majcher–Macyna–Zagórski.

Secure? I’m skeptical.

But maybe erasing more bits
will improve security.

Improved reader algorithm:
recompute e from $M(d, e)$
by linear algebra.

Insist on $M(0, \cdot)$ invertibility.

Improved algorithm allows
erasing many more bits.