Non-uniform cracks in the concrete

Daniel J. Bernstein
University of Illinois at Chicago

Joint work with:
Tanja Lange
Technische Universiteit Eindhoven

Paper coming soon,
including detailed credits
and historical discussion.

Classic “concrete security”
metric for cipher insecurity:

“The maximum,
over all adversaries
restricted to q' input-output
examples and execution time t',
of the ‘advantage’
that the adversary has
in the game of distinguishing
[the cipher for a secret key]
from a random permutation.”

Attractive theorems: e.g.,
“$\mathbf{Adv}^{\mathrm{prf}}_{\mathrm{CBC}^m\text{-}F}(q,t) \le$
$\mathbf{Adv}^{\mathrm{prp}}_{F}(q',t') + \dfrac{q^2m^2}{2^{l-1}}$
where $q' = mq$
and $t' = t + O(mql)$.”

Attractive theorems: e.g.,
"$\mathbf{Adv}^{\text{prf}}_{\text{CBC}^m\text{-}F}(q,t) \le \mathbf{Adv}^{\text{prp}}_{F}(q',t') + \frac{q^2m^2}{2^{l-1}}$
where $q' = mq$
and $t' = t + O(mql)$."

Conjectured bounds on
insecurity of specific ciphers
that have survived cryptanalysis:
e.g., "$\mathbf{Adv}^{\text{prp}-\text{cpa}}_{\text{AES}}(\cdots) \le c_1 \cdot \frac{t/T_{\text{AES}}}{2^{128}} + c_2 \cdot \frac{q}{2^{128}}$."

Similar public-key story.

Define t-insecurity of RSA-1024 as maximum success probability of all attacks that cost $\leq t$.

Similar public-key story.

Define t-insecurity of RSA-1024 as maximum success probability of all attacks that cost $\leq t$.

Prove, e.g., that bounds on insecurity of RSA-1024 imply similar bounds on insecurity of RSA-1024-PSS.

Similar public-key story.

Define t-insecurity of RSA-1024 as maximum success probability of all attacks that cost $\leq t$.

Prove, e.g., that bounds on insecurity of RSA-1024 imply similar bounds on insecurity of RSA-1024-PSS.

Conjecture bounds on insecurity of RSA-1024: e.g., "it takes time $Ce^{1.923(\log N)^{1/3}(\log\log N)^{2/3}}$ to invert RSA".

These conjectures are wrong.

There *exist* algorithms breaking AES, RSA-3072, DSA-3072, and ECC-256 at cost far below 2^{128}; e.g., time 2^{85} to break ECC-256. (Assuming standard heuristics.)

These conjectures are wrong.

There *exist* algorithms breaking AES, RSA-3072, DSA-3072, and ECC-256 at cost far below 2^{128}; e.g., time 2^{85} to break ECC-256. (Assuming standard heuristics.)

No actual security problem: *Finding* these algorithms costs more than 2^{128}.

These conjectures are wrong.

There *exist* algorithms breaking AES, RSA-3072, DSA-3072, and ECC-256 at cost far below 2^{128}; e.g., time 2^{85} to break ECC-256. (Assuming standard heuristics.)

No actual security problem: *Finding* these algorithms costs more than 2^{128}.

$\Rightarrow$ Very large separation between standard definition and actual insecurity.

These conjectures are wrong.

There *exist* algorithms breaking AES, RSA-3072, DSA-3072, and ECC-256 at cost far below 2^{128}; e.g., time 2^{85} to break ECC-256. (Assuming standard heuristics.)

No actual security problem: *Finding* these algorithms costs more than 2^{128}.

$\Rightarrow$ Very large separation between standard definition and actual insecurity.

Undermines concrete-security evaluations and comparisons.

Several possible fixes,
all causing trouble. Examples:

Several possible fixes,
all causing trouble. Examples:

1. Add enough uniformity.
Clearly stops attacks.
Requires massive rewrite
of theorems in literature.
Abandons goal of defining concrete security of AES.

Several possible fixes,
all causing trouble. Examples:

1. Add enough uniformity.
Clearly stops attacks.
Requires massive rewrite
of theorems in literature.
Abandons goal of defining concrete security of AES.

2. Switch to AT metric.
Preserves goal of defining
concrete security of AES.
Seems to stop all attacks
above reasonable Pr cutoff.
Breaks more theorems.