The fundamental goal of "provable security"

D. J. Bernstein

University of Illinois at Chicago &
Technische Universiteit Eindhoven

Let's focus on what "provable security" is trying to do.

Let's not get distracted by current obstacles: proof errors, looseness, limited models, etc. Surely these can all be fixed.

Let's look at an example . . .

Chaum–van Heijst–Pfitzmann, Crypto 1991: choose p sensibly; define $C(x, y) = 4^x 9^y \bmod p$ for suitable ranges of x and y.

Simple, beautiful, structured.

Very easy security reduction: finding C collision implies computing a discrete logarithm.

Chaum–van Heijst–Pfitzmann, Crypto 1991: choose p sensibly; define $C(x, y) = 4^x 9^y \bmod p$ for suitable ranges of x and y.

Simple, beautiful, structured.

Very easy security reduction: finding C collision implies computing a discrete logarithm.

Typical exaggerations: C is "provably secure"; C is "cryptographically collision-free"; "security follows from rigorous mathematical proofs".

This is very bad cryptography.
Horrible security for its speed.
Far worse security record than
“unstructured” compression-
function designs such as BLAKE.

This is very bad cryptography.
Horrible security for its speed.
Far worse security record than
"unstructured" compression-
function designs such as BLAKE.

How did we figure this out?
Cryptanalysis!

Security losses in C include
1922 Kraitchik (index calculus);
1986 Coppersmith–Odlyzko–
Schroeppel (NFS predecessor);
1993 Gordon (general DL NFS);
1993 Schirokauer (faster NFS);
1994 Shor (quantum poly time).

A security reduction can be
a useful guide *to cryptanalysts*:
"to attack C, focus on DL."

A security reduction can be
a useful guide *to cryptanalysts*:
"to attack C, focus on DL."

But if you advertise
the "provable security" of C
to cryptographic users then
you're a snake-oil salesman.

"Provable security" has very little
correlation with actual security,
maybe even negative correlation:
C's structure **helps the proof**
but also helps attackers.

"If it's provably secure, it's
probably not" —Lars Knudsen

Not everyone agrees:

"The only reasonable approach is to construct cryptographic systems with the objective of being able to give security reductions." —Ivan Damgård

Not everyone agrees:
"The only reasonable approach is to construct cryptographic systems with the objective of being able to give security reductions." —Ivan Damgård

This approach produces papers but does not produce security.

From a security perspective, the only reasonable objective is to construct cryptographic systems *that will survive cryptanalysis*.

Users should select cryptographic systems *based on cryptanalysis*.