How to Eat Your Entropy and Have It Too
(Recovering from compromise)

Yevgeniy Dodis
Adi Shamir
Noah Stephens-Davidowitz
Daniel Wichs
Our Goal
Our Goal

figure 1a: Having
Our Goal

figure 1a: Having

figure 1b: Eating it too
Our Goal

**figure 1a:** Having

**figure 1b:** Eating it too
How Does TCC Build a PRG?
How Does TCC Build a PRG?
How Does TCC Build a PRG?

\[ S_0 \xrightarrow{PRG} S_1 \xrightarrow{PRG} S_2 \]

\[ R_0 \quad R_1 \]
How Does TCC Build a PRG?

\[ S_0 \xrightarrow{\text{PRG}} S_1 \xrightarrow{\text{PRG}} S_2 \xrightarrow{\text{PRG}} S_3 \]

\[ R_0 \]
\[ R_1 \]
\[ R_2 \]
How Does TCC Build a PRG?

Perfect randomness…
Developers Build
“RNGs with Input”
Developers Build
“RNGs with Input”
Developers Build
“RNGs with Input”

\[ S \xrightarrow{\text{next}} S', R \]

\[ S, I \xrightarrow{\text{refresh}} S' \]
Developers Build
“RNGs with Input”

\[ S \xrightarrow{\text{next}} S', R \]

\[ S, I \xrightarrow{\text{refresh}} S' \]

Entropy?
Developers Build
“RNGs with Input”

\[ S \xrightarrow{\text{next}} S', R \]

\[ S, I \xrightarrow{\text{refresh}} S' \]

Entropy?

Accumulated entropy
Developers Build
“RNGs with Input”

\[ S \xrightarrow{\text{next}} S', R \]

\[ S, I \xrightarrow{\text{refresh}} S' \]

Entropy?

Accumulated entropy

\[ H(S') \approx H(S) + H(I) \]
(Limited) Formal Analysis

[BH05] [DPRVW13]
(Limited) Formal Analysis

First formal model (In 2005!)

[BH05] [DPRVW13]
(Limited) Formal Analysis

First formal model (In 2005!)

Recover only after full-entropy input

[BH05] [DPRVW13]
(Limited) Formal Analysis

First formal model (In 2005!)

Recover only after full-entropy input

Gathers entropy as it comes

[BH05]

[ DPRVW13 ]
(Limited) Formal Analysis

[BH05]

First formal model (in 2005!)

Recover only after full-entropy input

[DPREW13]

Gathers entropy as it comes

But....
Premature Next

RNG with input
Premature Next

RNG with input
Premature Next

RNG with input
Premature Next

RNG
with input
Premature Next

RNG with input
Premature Next

RNG
with input

leftrightarrow
leftrightarrow
Premature Next

RNG with input
Premature Next

RNG with input
Premature Next

RNG with input

I

I

I
Premature Next

RNG with input
Premature Next

RNG with input
Premature Next

RNG with input
Premature Next

RNG
with input

→

Dice
Premature Next

RNG with input

R →

I ←
Premature Next

S

RNG with input

R

I
Premature Next

RNG with input
How do we deal with this?
Option 1: Don’t Let The Adversary Look

RNG
with input
Option 1: Don’t Let The Adversary Look
Option 1: Don’t Let The Adversary Look
Option 1: Don’t Let The Adversary Look

RNG with input
Option 1: Don’t Let The Adversary Look

RNG with input
Option 1: Don’t Let The Adversary Look

RNG with input
Option 1: Don’t Let The Adversary Look
Option 1: Don’t Let The Adversary Look
Option 1: Don’t Let The Adversary Look
Option 2: Estimate Entropy

RNG
with input
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy
Option 2: Estimate Entropy
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy
Option 2: Estimate Entropy

RNG with input
Option 2: Estimate Entropy

RNG with input

? → R

? → ?

? → ?

I → I

I → ...

I → I

I → I
Option 2: Estimate Entropy

But we can’t estimate entropy....
Option 3: Prove Impossibility
Option 3: Prove Impossibility

But it’s possible....
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too

[Diagram with a character and dice]
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too
Option 4: Eat Your Entropy and Have It Too

Adi Shamir
Idea Used in Practice (but not theory…)

[KSF99]’s Yarrow  [FS03]’s Fortuna
Idea Used in Practice (but not theory...)

Only two pools

[KSF99]'s Yarrow [FS03]'s Fortuna
Idea Used in Practice
(but not theory…)

Only two pools

[KSF99]’s Yarrow

Many pools with clever scheduling

[FS03]’s Fortuna
Idea Used in Practice (but not theory…)

Only two pools

[KSF99]'s Yarrow

Many pools with clever scheduling

[FS03]'s Fortuna

OS X  iOS

FreeBSD®
Idea Used in Practice (but not theory…)

Only two pools

[KSF99]'s Yarrow

Many pools with clever scheduling

[FS03]'s Fortuna

OS X  iOS  FreeBSD®

Windows® 8
Our Work
Our Work

• Formal model (very strong security notion)
Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)
Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)
- Attacks on prior constructions
Our Work

- Formal model (very strong security notion)
- Provably secure construction in this model
  - Inspired by Fortuna
  - Proof in standard model (from OWF)
- Attacks on prior constructions
- Formal analysis of and improvement of Fortuna
  - Secure in limited setting
  - Doubled entropy efficiency
Thanks!

OMG! YAY! CAKE!

I'm totally gonna eat you too!