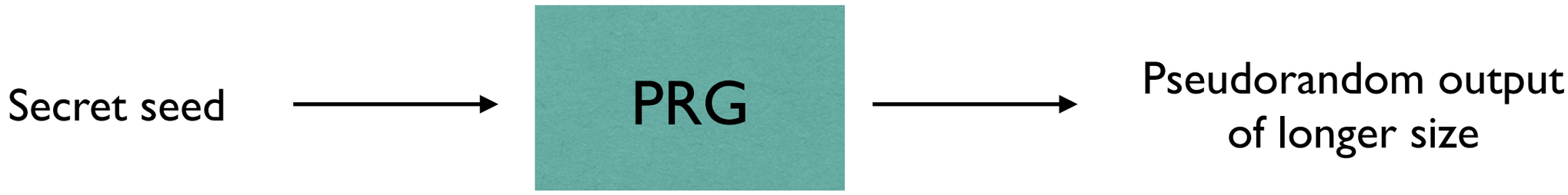
On the Concrete Security of Goldreich's Pseudorandom Generator

Geoffroy Couteau - Aurélien Dupin - Pierrick Méaux - Mélissa Rossi - Yann Rotella

ASIACRYPT

2018/12/04

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)



Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

Secret seed → **PRG** → Pseudorandom output of longer size

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

x_1

x_2

x_3

$\vdots$

x_n

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

Secret seed → **PRG** → Pseudorandom output of longer size

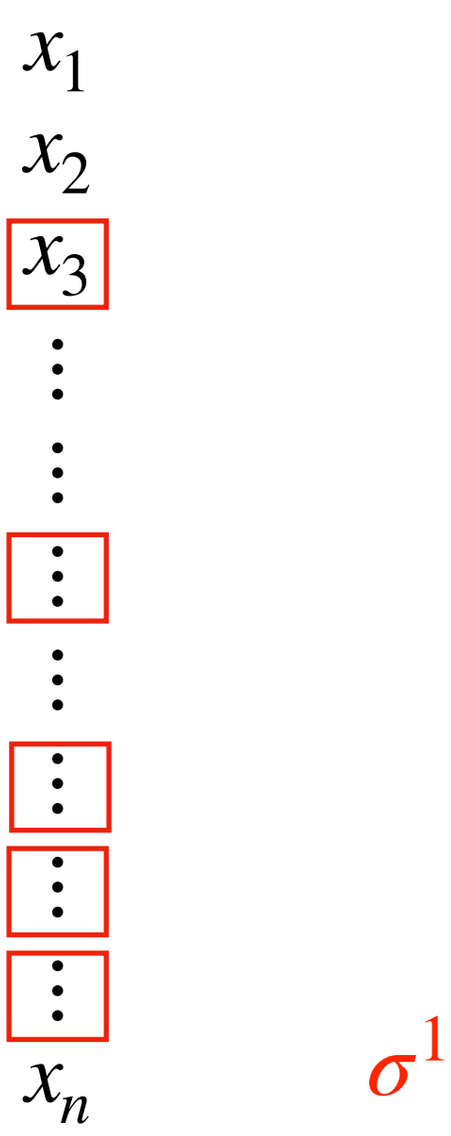
$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$



Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

Secret seed → PRG → Pseudorandom output of longer size

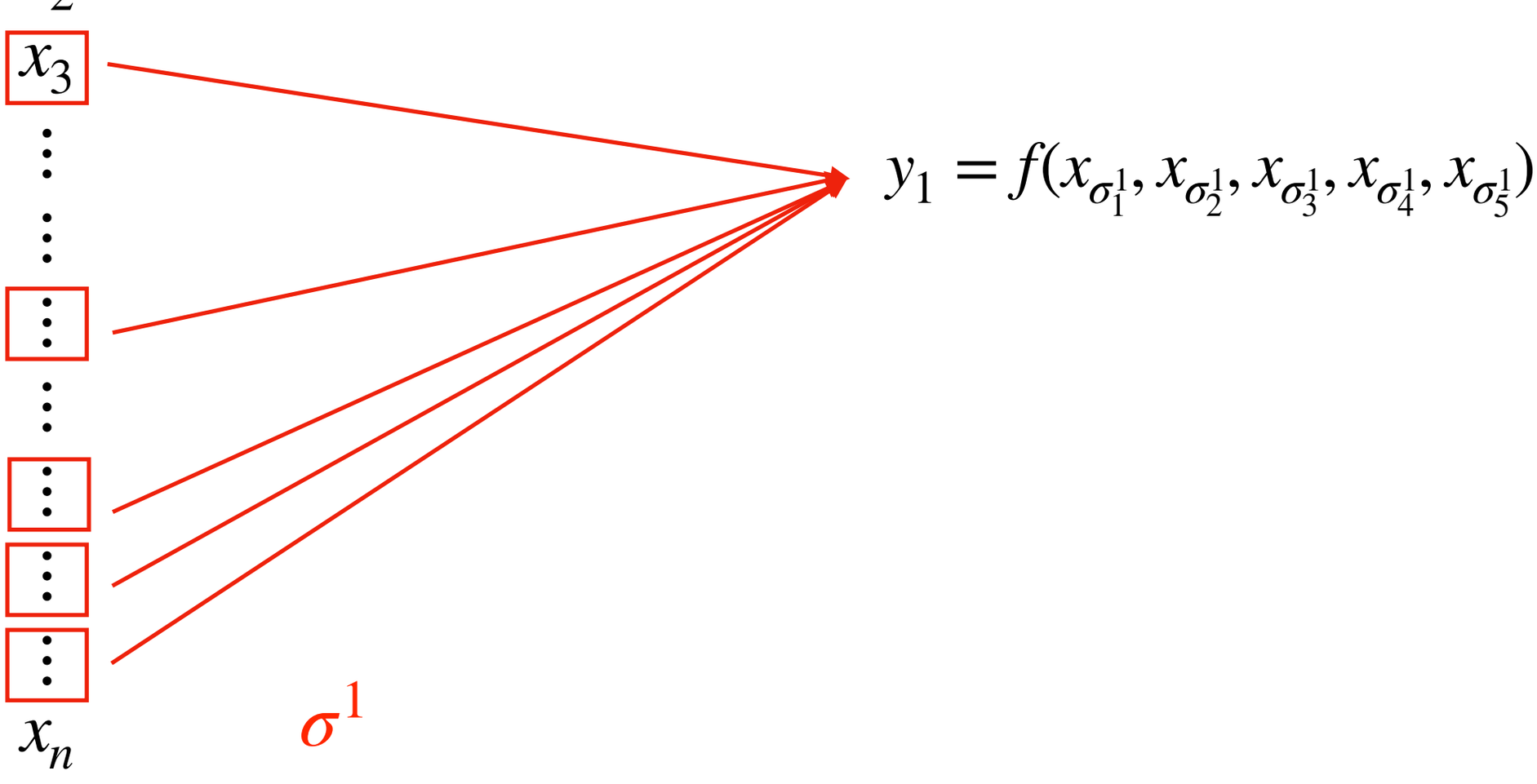
$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$



Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

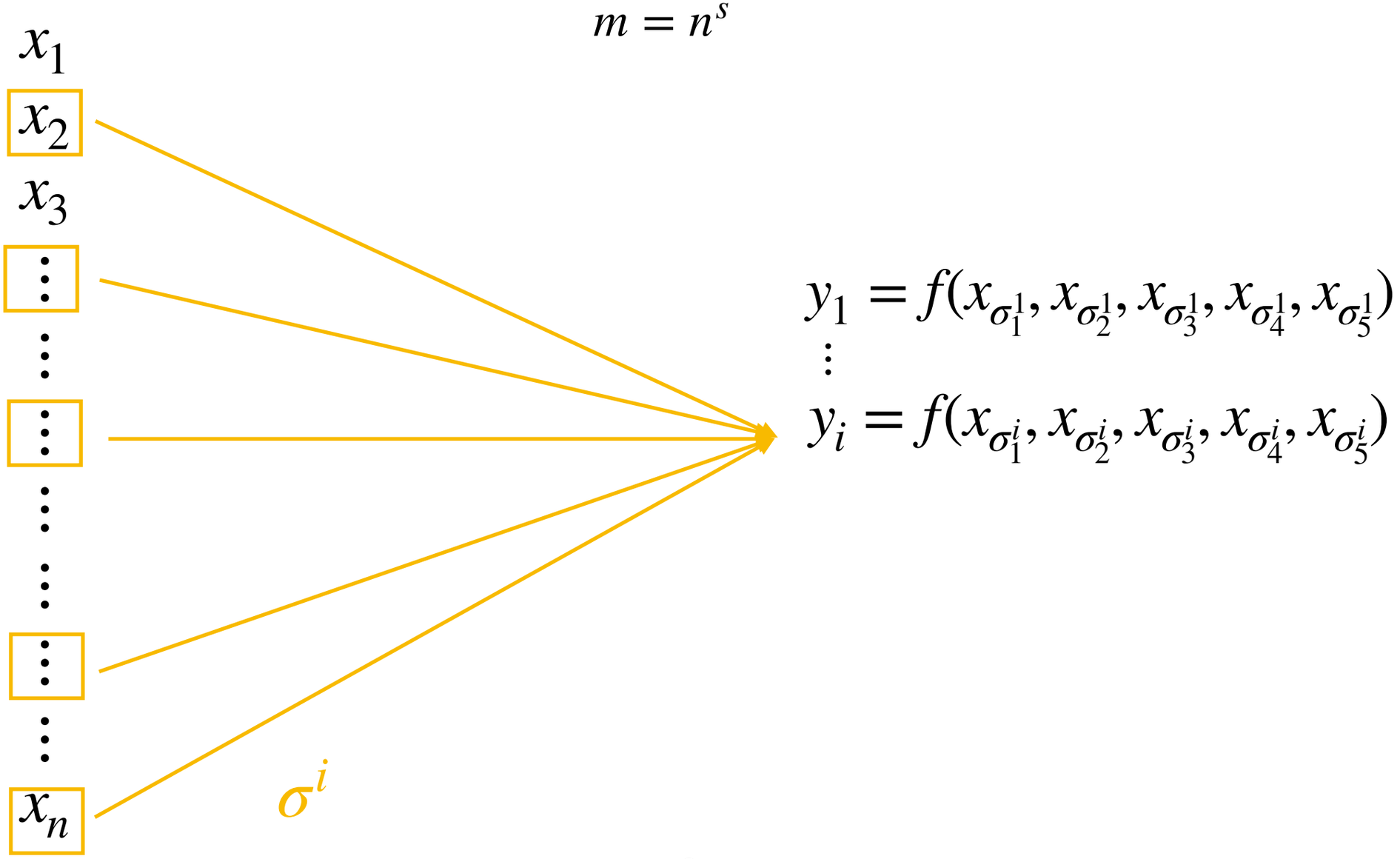
Secret seed → **PRG** → Pseudorandom output of longer size

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$



$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

Secret seed → PRG → Pseudorandom output of longer size

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

$$y_1 = f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1})$$
$$\vdots$$
$$y_i = f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i})$$
$$\vdots$$
$$y_m = f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})$$

Public system

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Parameters (n, s)

Stretch $s > 1$

$m = n^s$

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Locality Cardinality of the subsets

- Here the locality is 5

$$y_1 = f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1})$$
$$\vdots$$
$$y_i = f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i})$$
$$\vdots$$
$$y_m = f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})$$

Public system

Goldreich Pseudorandom Generator (Goldreich TOCT 2000)

Locality Cardinality of the subsets

- Here the locality is 5

$$y_1 = f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1})$$
$$\vdots$$
$$y_i = f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i})$$
$$\vdots$$
$$y_m = f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})$$

Public system

Predicate Function f

Boolean function of low degree

Goldreich Pseudorandom Generator

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Secret seed

$$
\begin{aligned}
y_1 &= f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1}) \\
&\vdots \\
y_i &= f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) \\
&\vdots \\
y_m &= f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})
\end{aligned}
$$

Public system

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Public output

Goldreich Pseudorandom Generator

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Secret seed

$$
\begin{aligned}
y_1 &= f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1}) \\
&\vdots \\
y_i &= f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) \\
&\vdots \\
y_m &= f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})
\end{aligned}
$$

Public system

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Public output

Security properties Consider a uniformly random secret seed

1. **Pseudorandomness**

   $(y_1, y_2, \ldots y_m)$ is indistinguishable from uniform

Goldreich Pseudorandom Generator

$x_1, x_2, \ldots x_n \in \mathbb{F}_2$

Secret seed

$$
\begin{aligned}
y_1 &= f(x_{\sigma_1^1}, x_{\sigma_2^1}, x_{\sigma_3^1}, x_{\sigma_4^1}, x_{\sigma_5^1}) \\
&\vdots \\
y_i &= f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) \\
&\vdots \\
y_m &= f(x_{\sigma_1^m}, x_{\sigma_2^m}, x_{\sigma_3^m}, x_{\sigma_4^m}, x_{\sigma_5^m})
\end{aligned}
$$

Public system

$y_1, y_2, \ldots y_m \in \mathbb{F}_2$

Public output

Security properties Consider a uniformly random secret seed

1. **Pseudorandomness**

   $(y_1, y_2, \ldots y_m)$ is indistinguishable from uniform

2. **One wayness**

   Knowing the system and output, the probability to recover the seed is negligible

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Mossel, Shpilka, Trevisan FOCS 2003

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Security study

Mossel, Shpilka, Trevisan FOCS 2003

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

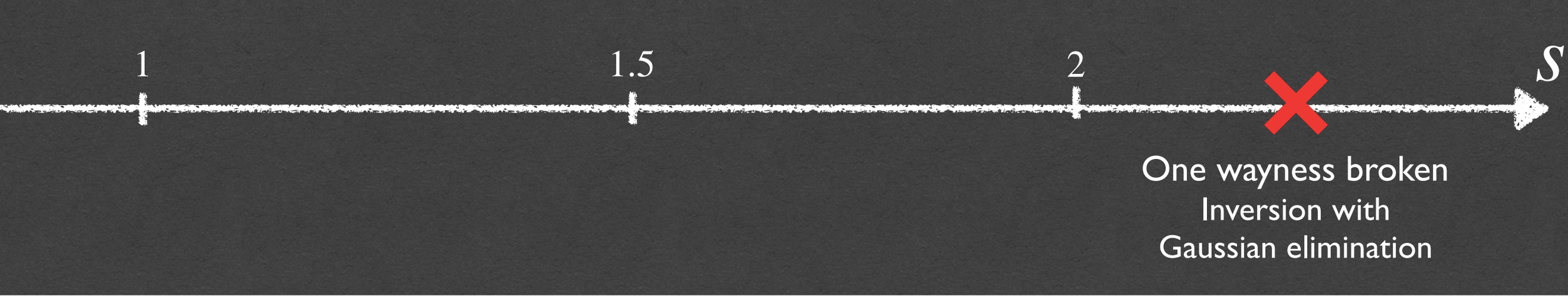
Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Security study



Mossel, Shpilka, Trevisan FOCS 2003

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

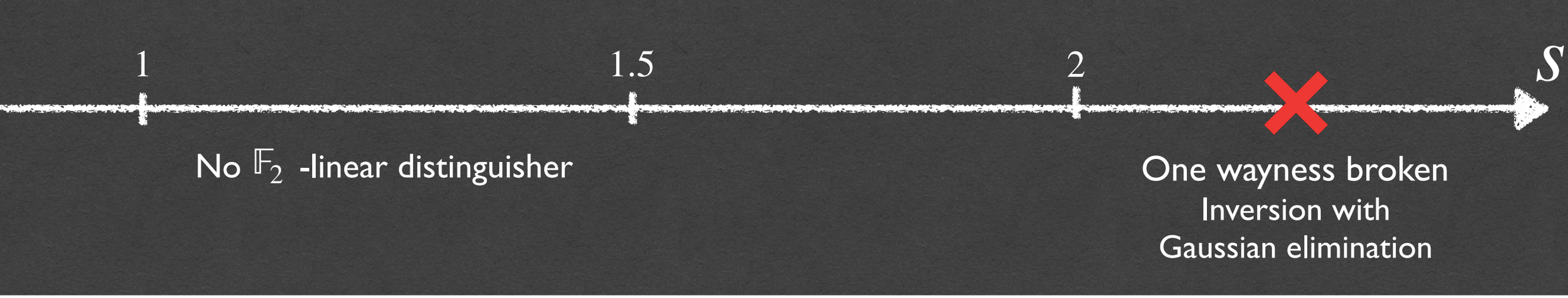
Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Security study



Mossel, Shpilka, Trevisan FOCS 2003
O'Donnel Witmer CCC 2014
Applebaum, Bogdanov, Rosen TCC 2012

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

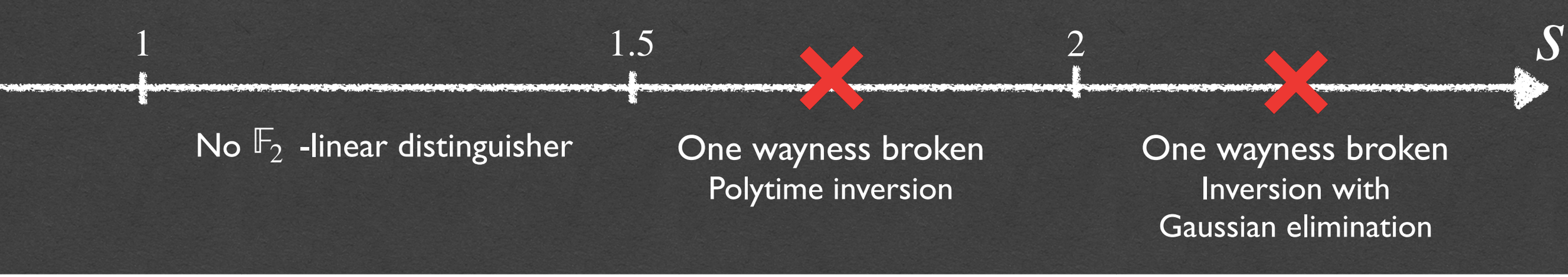
Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Security study



Mossel, Shpilka, Trevisan FOCS 2003
O'Donnel Witmer CCC 2014
Applebaum, Bogdanov, Rosen TCC 2012
Applebaum TCC 2013

Predicate P5

$$f(x_{\sigma_1^i}, x_{\sigma_2^i}, x_{\sigma_3^i}, x_{\sigma_4^i}, x_{\sigma_5^i}) = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$

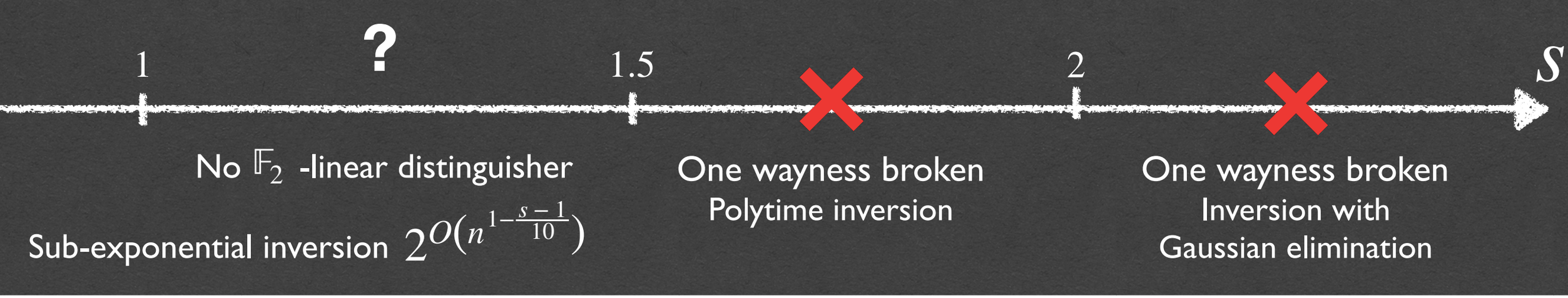
Predicate P5

- Smallest locality 5
- Algebraic degree 2
- Algebraic immunity 2

$$m = n^s$$

$$s > 1$$

Security study



Mossel, Shpilka, Trevisan FOCS 2003
O'Donnel Witmer CCC 2014
Applebaum, Bogdanov, Rosen TCC 2012
Applebaum TCC 2013
Bogdanov, Qiao ARCO 2009

Theoretical applications of Goldreich's PRG

Theoretical applications of Goldreich's PRG

Semi Secure computation with constant computational overhead

Ishai *et al.* STOC 2008
Applebaum *et al.* CRYPTO 2017

Goldreich Pseudorandom Generator

Theoretical applications of Goldreich's PRG

Semi Secure computation with constant computational overhead

Ishai *et al.* STOC 2008
Applebaum *et al.* CRYPTO 2017

Indistinguishability Obfuscation

Sahai and Waters STOC 2014
Lin and Tessaro CRYPTO 2017

Goldreich Pseudorandom Generator

Theoretical applications of Goldreich's PRG

Semi Secure computation with constant computational overhead

Ishai *et al.* STOC 2008
Applebaum *et al.* CRYPTO 2017

Indistinguishability Obfuscation

Sahai and Waters STOC 2014
Lin and Tessaro CRYPTO 2017

Goldreich Pseudorandom Generator

MPC-friendly primitives

Albrecht *et al.* EUROCRYPT 2015
Canteaut *et al.* FSE 2016
Méaux *et al.* EUROCRYPT 2016
Grassi *et al.* ACM-CCS 2016

Theoretical applications of Goldreich's PRG

Semi Secure computation with constant computational overhead

Ishai *et al.* STOC 2008
Applebaum *et al.* CRYPTO 2017

Indistinguishability Obfuscation

Sahai and Waters STOC 2014
Lin and Tessaro CRYPTO 2017

Goldreich Pseudorandom Generator

MPC-friendly primitives

Albrecht *et al.* EUROCRYPT 2015
Canteaut *et al.* FSE 2016
Méaux *et al.* EUROCRYPT 2016
Grassi *et al.* ACM-CCS 2016

Cryptographic capsules

Boyle *et al.* ACM-CCS 2017

Our first contribution

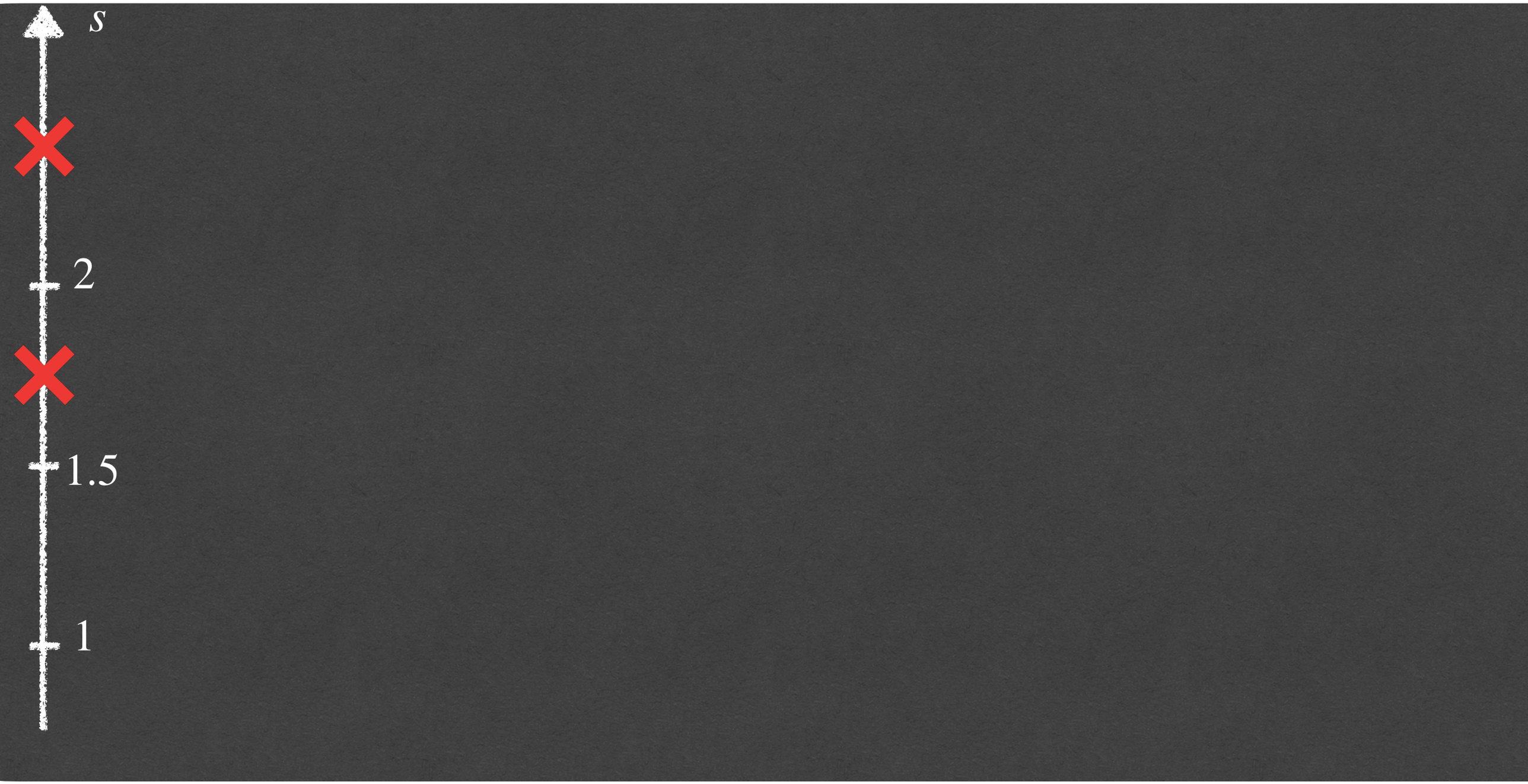
New attacks

with a more fine-grained complexity estimation

Our first contribution

New attacks

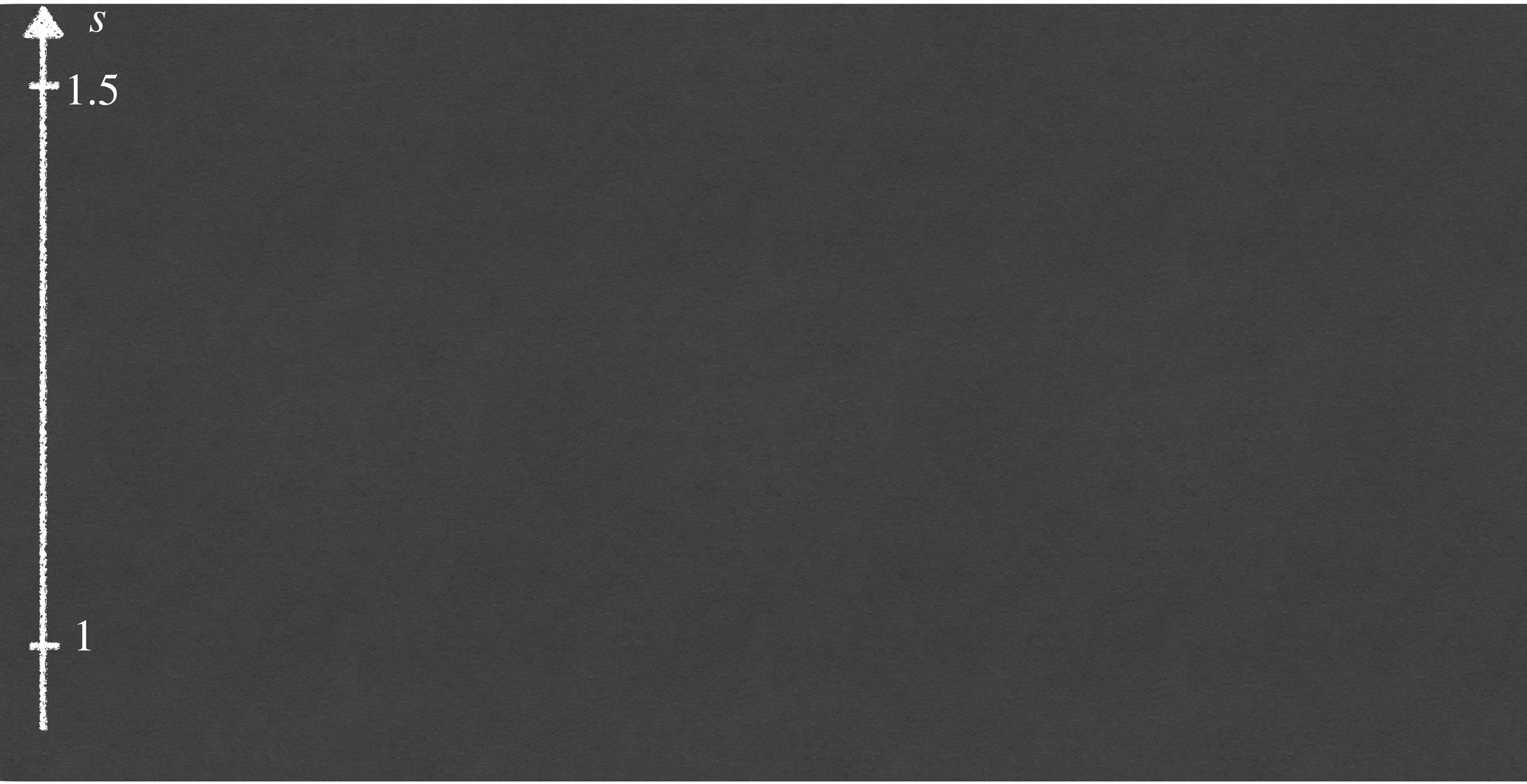
with a more fine-grained complexity estimation



Our first contribution

New attacks

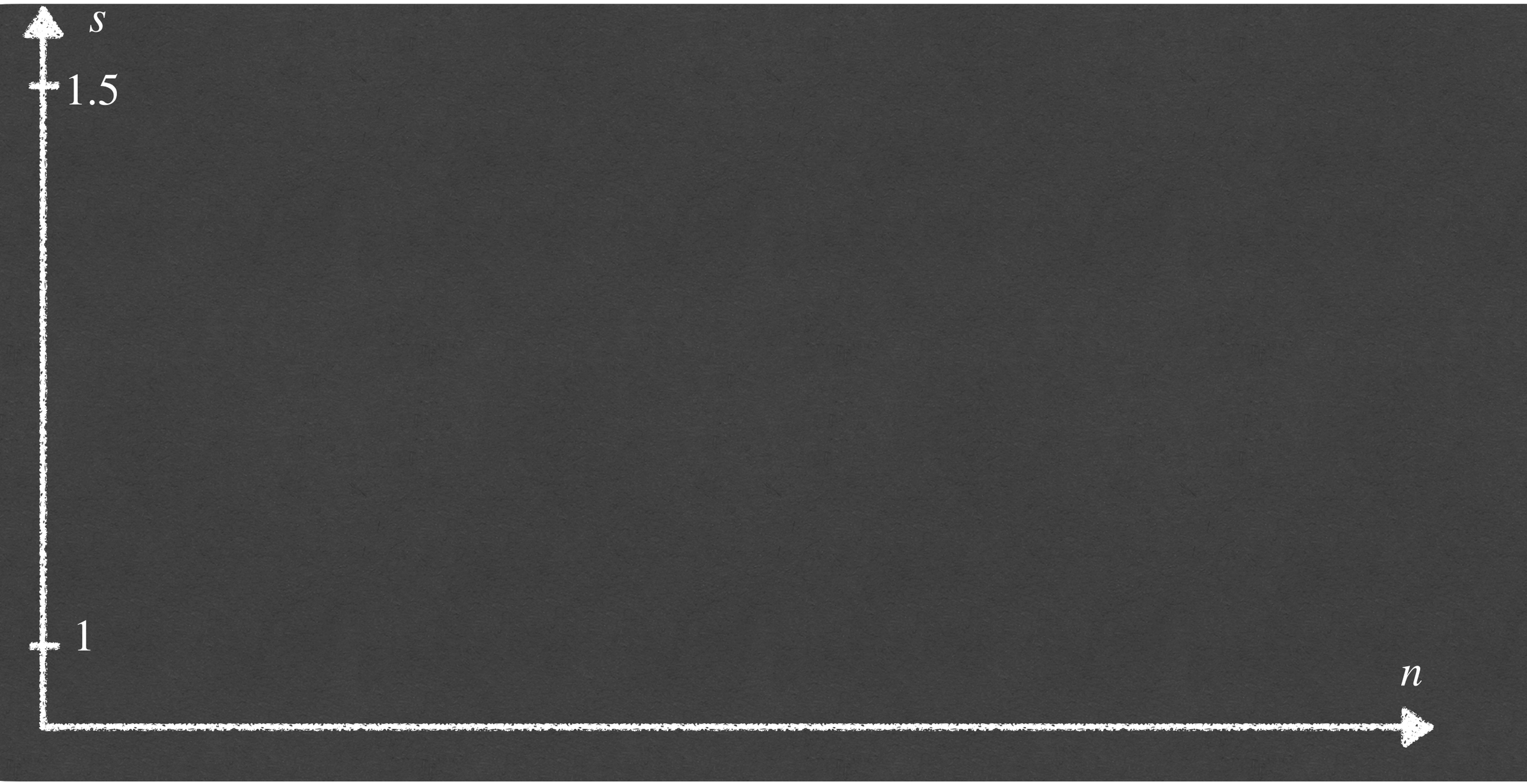
with a more fine-grained complexity estimation



Our first contribution

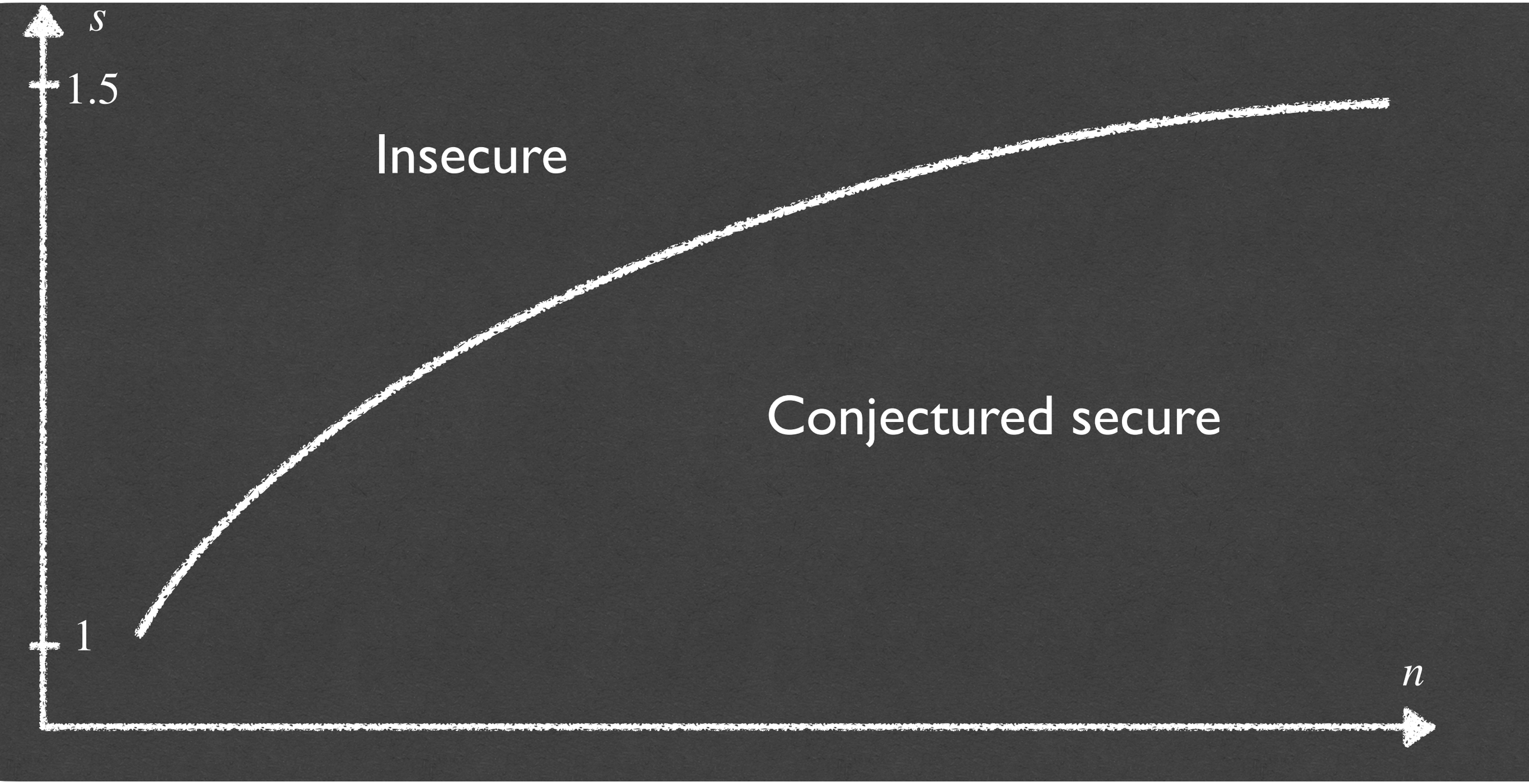
New attacks

with a more fine-grained complexity estimation



Our first contribution

New attacks
with a more fine-grained complexity estimation



Outline

Guess-and-Determine attack

1. Collisions : linear equations for free

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Guess-and-Determine attack

1. Collisions : linear equations for free

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Guess-and-Determine attack

1. Collisions : linear equations for free

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

$$x_3 + x_9 + x_2 + x_5x_1 + x_{17} + x_2 + x_1 + x_5x_1 = 1 + 1$$

$$x_3 + x_9 + x_2 + x_{17} + x_2 + x_1 = 0$$

Guess-and-Determine attack

1. Collisions : linear equations for free

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

$$x_3 + x_9 + x_2 + x_5x_1 + x_{17} + x_2 + x_1 + x_5x_1 = 1 + 1$$

$$x_3 + x_9 + x_2 + x_{17} + x_2 + x_1 = 0$$

Average number of collisions

$$\mathbb{E}(c) = m - \binom{n}{2} + \binom{n}{2}\left(\frac{\binom{n}{2} - 1}{\binom{n}{2}}\right)^m \in O(n^{2(s-1)})$$

Guess-and-Determine attack

1. Collisions : linear equations for free

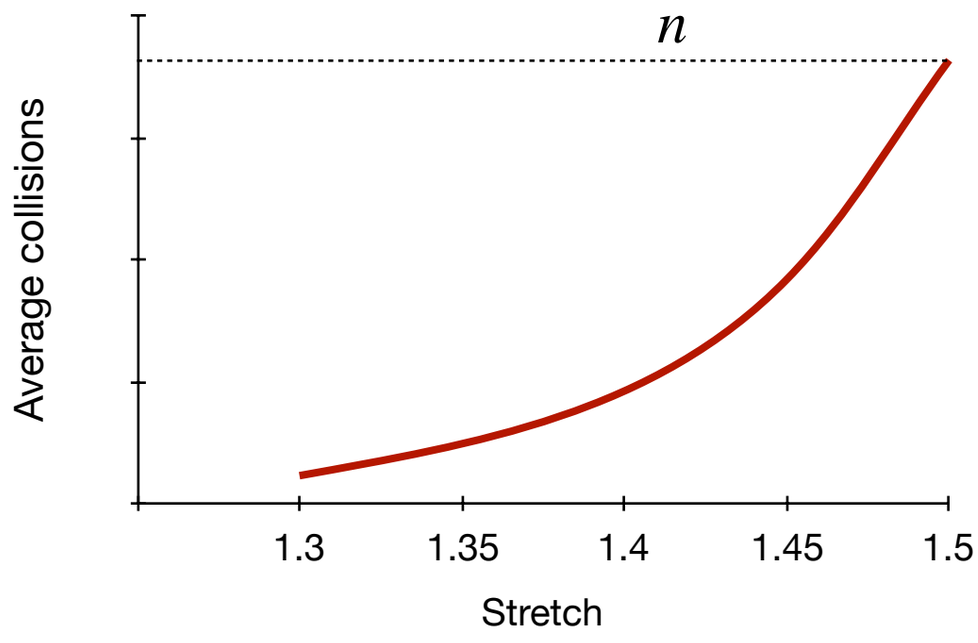
$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

$$x_3 + x_9 + x_2 + x_5x_1 + x_{17} + x_2 + x_1 + x_5x_1 = 1 + 1$$

$$x_3 + x_9 + x_2 + x_{17} + x_2 + x_1 = 0$$

Average number of collisions

$$\mathbb{E}(c) = m - \binom{n}{2} + \binom{n}{2}\left(\frac{\binom{n}{2} - 1}{\binom{n}{2}}\right)^m \in O(n^{2(s-1)})$$



Guess-and-Determine attack

2 Complete the linear system obtained with guesses

$$\begin{cases} x_3 + x_9 + x_2 + x_5 x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15} x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14} x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5 x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6 x_5 = 1 \end{cases}$$

Guess-and-Determine attack

2 Complete the linear system obtained with guesses

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Guess-and-Determine attack

2 Complete the linear system obtained with guesses

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Guessing creates linear equations

Try $x_6 = 0$ and $x_6 = 1$

Guess-and-Determine attack

2 Complete the linear system obtained with guesses

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Guessing creates linear equations

Try $x_6 = 0$ and $x_6 = 1$

Average number of necessary guesses

$$\left\lfloor \frac{n(n-c)}{2(m-c)+n} + 1 \right\rfloor \simeq O\left(\frac{n^{2-s}}{2}\right)$$

Guess-and-Determine attack

Idea introduced by Bettale PhD Thesis 2011

1. Derive all the collisions → Linear system Σ_1

Guess-and-Determine attack

Idea introduced by Bettale PhD Thesis 2011

1. Derive all the collisions → Linear system Σ_1

2. Compute a small subset $\mathcal{G}$ of guesses → Linear system Σ_2

   such that $|\Sigma_1| + |\Sigma_2| \gg n$

Guess-and-Determine attack

Idea introduced by Bettale PhD Thesis 2011

1. Derive all the collisions → Linear system Σ_1

2. Compute a small subset $\mathcal{G}$ of guesses → Linear system Σ_2

   such that $|\Sigma_1| + |\Sigma_2| \gg n$

3. Solve $\Sigma = \Sigma_1 \cup \Sigma_2$ for all elements in $\mathcal{G}$

   i.e. solve the system, find a candidate seed and check if it matches the public evaluation of the PRG.

Guess-and-Determine attack

Idea introduced by Bettale PhD Thesis 2011

1. Derive all the collisions → Linear system Σ_1

2. Compute a small subset $\mathcal{G}$ of guesses → Linear system Σ_2

   such that $|\Sigma_1| + |\Sigma_2| \gg n$

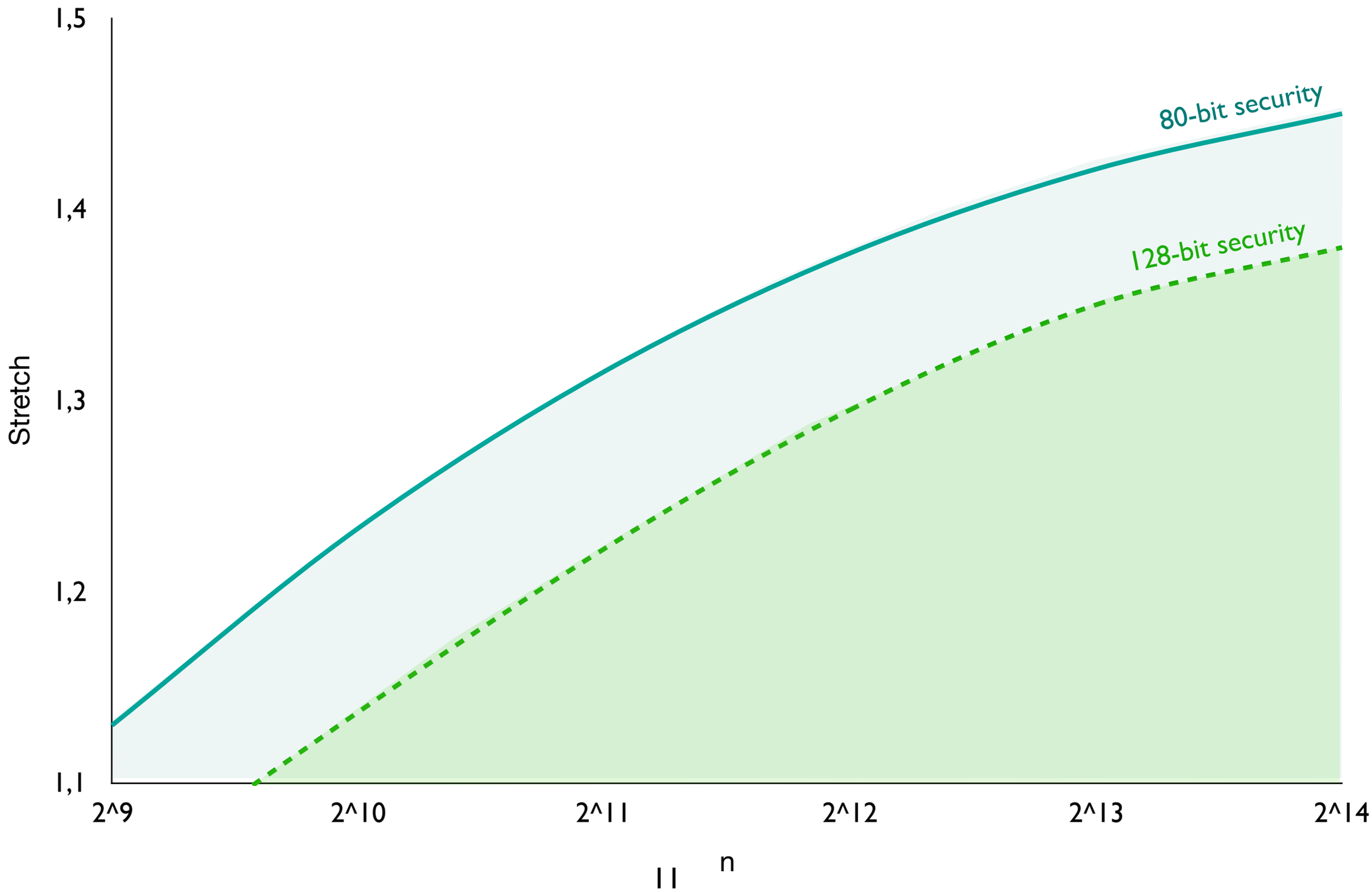
3. Solve $\Sigma = \Sigma_1 \cup \Sigma_2$ for all elements in $\mathcal{G}$

   i.e. solve the system, find a candidate seed and check if it matches the public evaluation of the PRG.

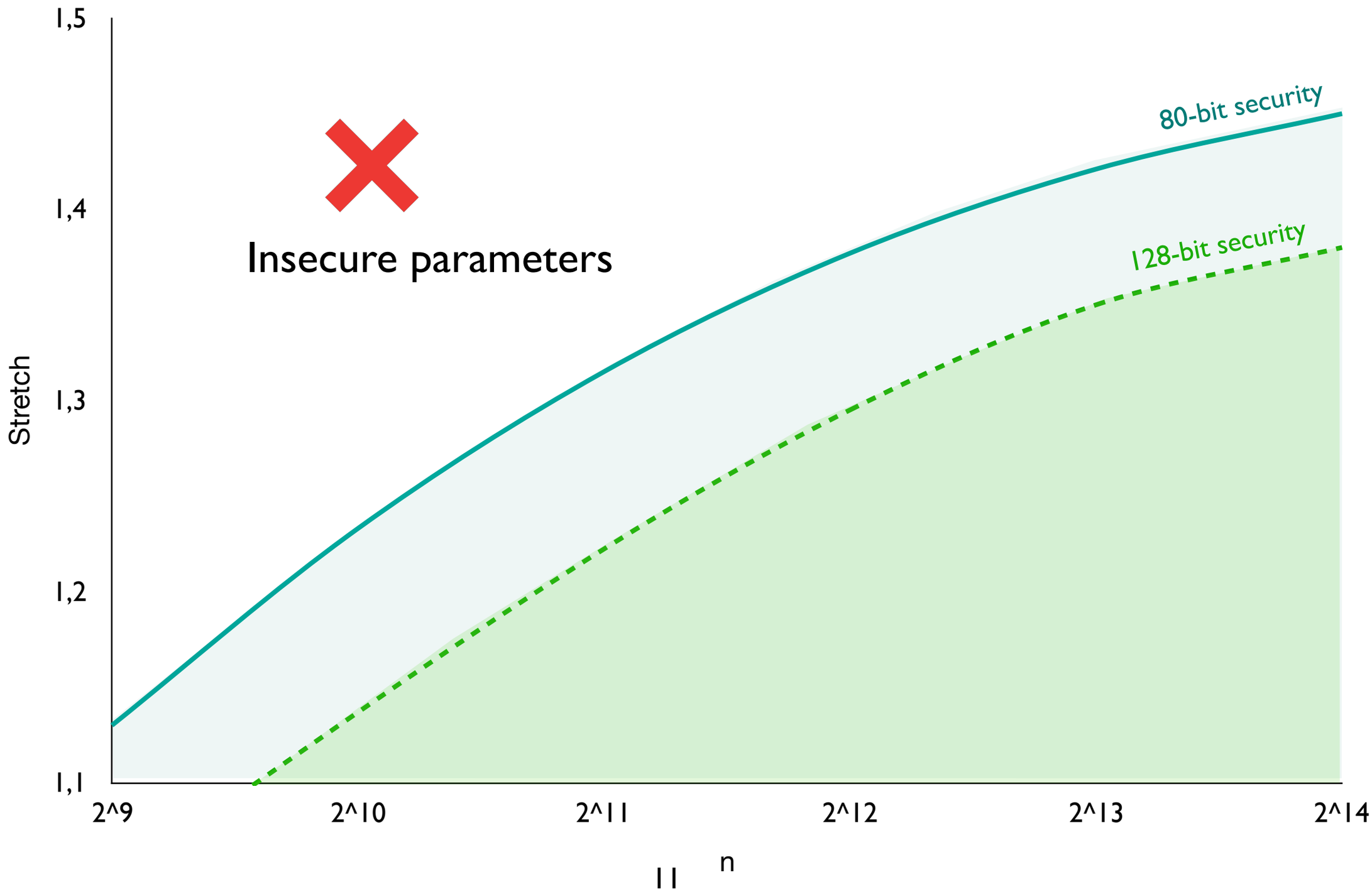
Total complexity $O\left(n^{\omega} 2^{\frac{n^2-s}{2}}\right)$

ω Exponent for solving linear systems

Guess-and-Determine attack



Guess-and-Determine attack

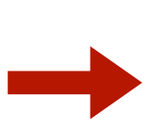


Outline

Degree-two attack

$$y_1 = x_{\sigma_1^1} + x_{\sigma_2^1} + x_{\sigma_3^1} + x_{\sigma_4^1} x_{\sigma_5^1}$$
$$\vdots$$
$$y_i = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$
$$\vdots$$
$$y_m = x_{\sigma_1^m} + x_{\sigma_2^m} + x_{\sigma_3^m} + x_{\sigma_4^m} x_{\sigma_5^m}$$

Public system



$$y_1 = x_{\sigma_1^1} + x_{\sigma_2^1} + x_{\sigma_3^1} + x_{\sigma_4^1} x_{\sigma_5^1}$$
$$\vdots$$
$$y_i = x_{\sigma_1^i} + x_{\sigma_2^i} + x_{\sigma_3^i} + x_{\sigma_4^i} x_{\sigma_5^i}$$
$$\vdots$$
$$y_m = x_{\sigma_1^m} + x_{\sigma_2^m} + x_{\sigma_3^m} + x_{\sigma_4^m} x_{\sigma_5^m}$$

Create many additional quadratic equations in order to be able to linearize

$$X_{i,j} \leftarrow x_i x_j$$

Degree-two attack

1. Create degree 2 equations

Degree-two attack

1. Create degree 2 equations

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

$\times x_5$ → $x_5(x_3 + x_9 + x_2 + x_1) = x_5$

$\times x_1$ → $x_1(x_3 + x_9 + x_2 + x_5) = x_1$

Each equation can create 2 more equations

Degree-two attack

1. Create degree 2 equations

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

$\times x_5$: $x_5(x_3 + x_9 + x_2 + x_1) = x_5$

$\times x_1$: $x_1(x_3 + x_9 + x_2 + x_5) = x_1$

Each equation can create 2 more equations

$$\begin{cases} x_3 + x_9 + x_2 + x_5x_1 = 1 \\ x_1 + x_8 + x_3 + x_{15}x_2 = 0 \\ x_4 + x_{10} + x_{12} + x_{14}x_6 = 0 \\ x_{17} + x_2 + x_1 + x_5x_1 = 1 \\ x_7 + x_1 + x_{11} + x_6x_5 = 1 \end{cases}$$

Semi collision S-polynomial

$\times x_6$, $\times x_1$:

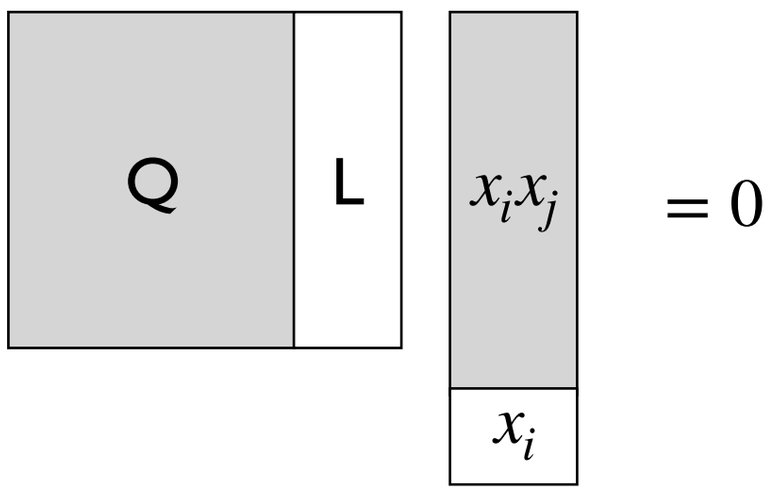
$$x_6(x_{17} + x_2 + x_1 + x_5x_1) + x_1(x_7 + x_1 + x_{11} + x_6x_5) = x_6 + x_1$$

$$x_6(x_{17} + x_2 + x_1) + x_1(x_7 + x_1 + x_{11}) = x_6 + x_1$$

Degree-two equation

Degree-two attack

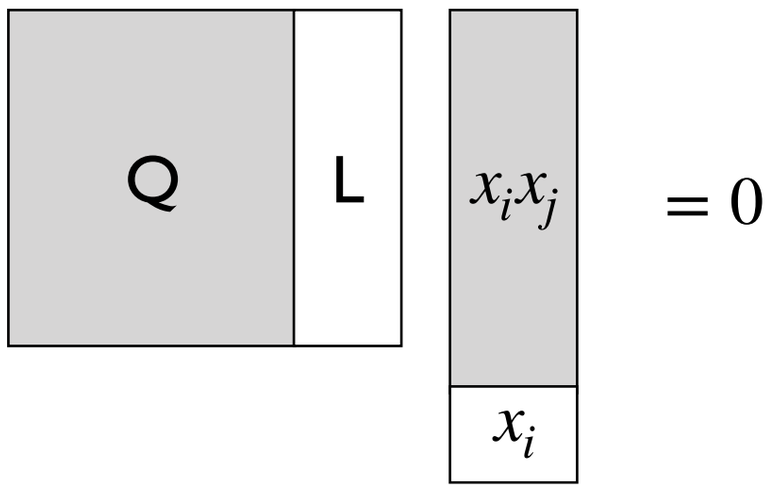
2 Try to solve $X_{i,j} \leftarrow x_i x_j$



→ Q and L are very sparse

Degree-two attack

2 Try to solve $X_{i,j} \leftarrow x_i x_j$

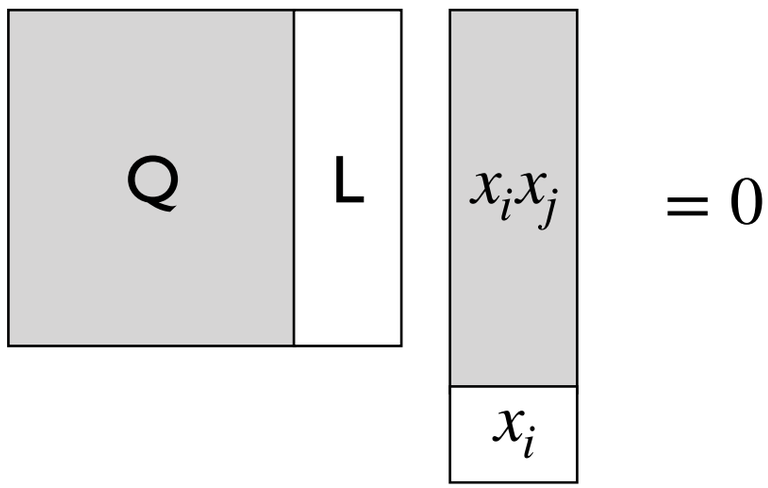


→ Q and L are very sparse

When $\mathcal{N}_{eq}(n, s) \approx \mathcal{N}_{var}(n)$, Q|L is full rank and the secret seed can be recovered

Degree-two attack

2 Try to solve $X_{i,j} \leftarrow x_i x_j$



→ Q and L are very sparse

When $\mathcal{N}_{eq}(n, s) \approx \mathcal{N}_{var}(n)$, Q|L is full rank and the secret seed can be recovered

Using heuristic assumptions (counting equations, linear independence), we were able to define a function f^* such that

$s \geq f(n) \implies$ the degree 2 attack succeeds with high probability

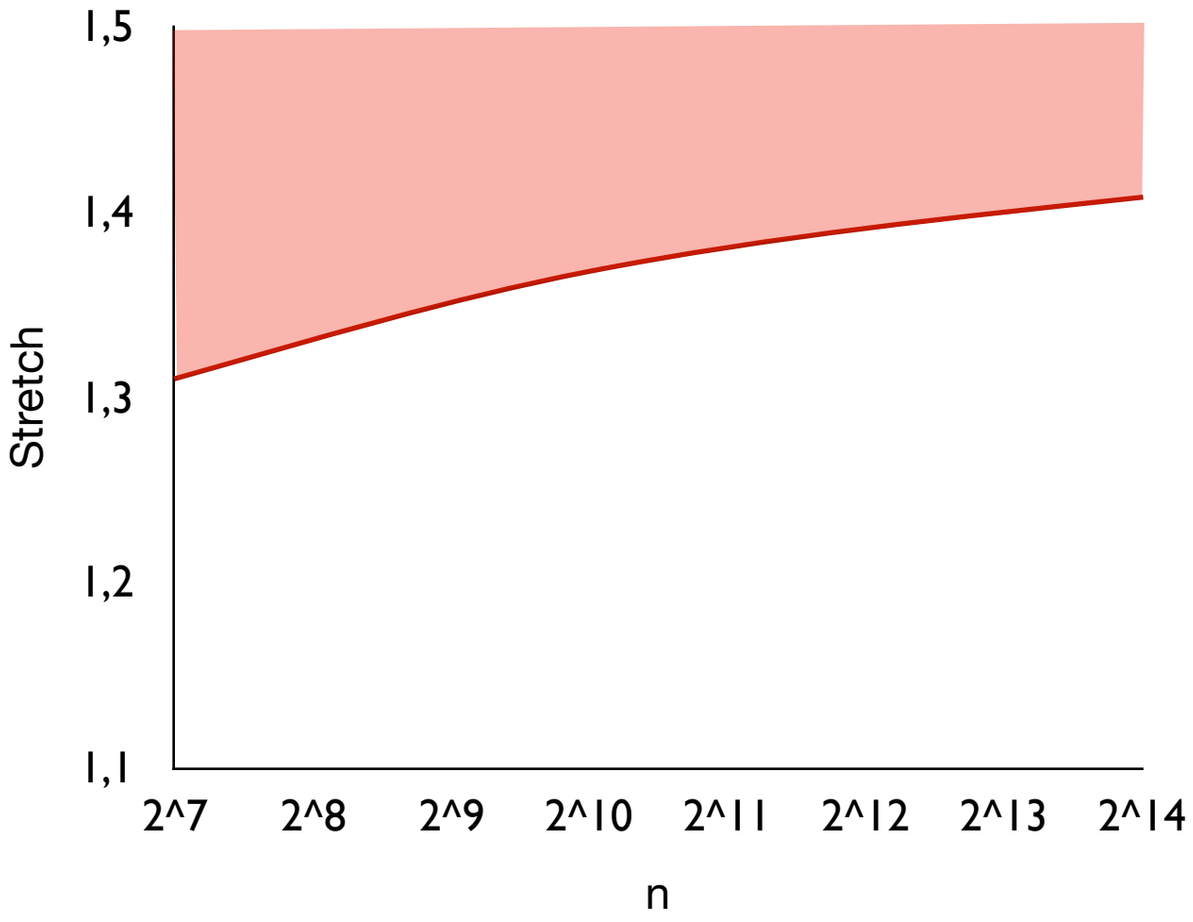
Conjectured degree 2 linearization (experimentally checked for small n)

*We thank Henri Gilbert and Guénaël Renault for helpful insights with this approach

Gröbner basis approach

Conjectured polynomial attack

For $s \geq f(n)$, the degree of regularity of the Gröbner basis computation is 3 with a degree 2 final resolution

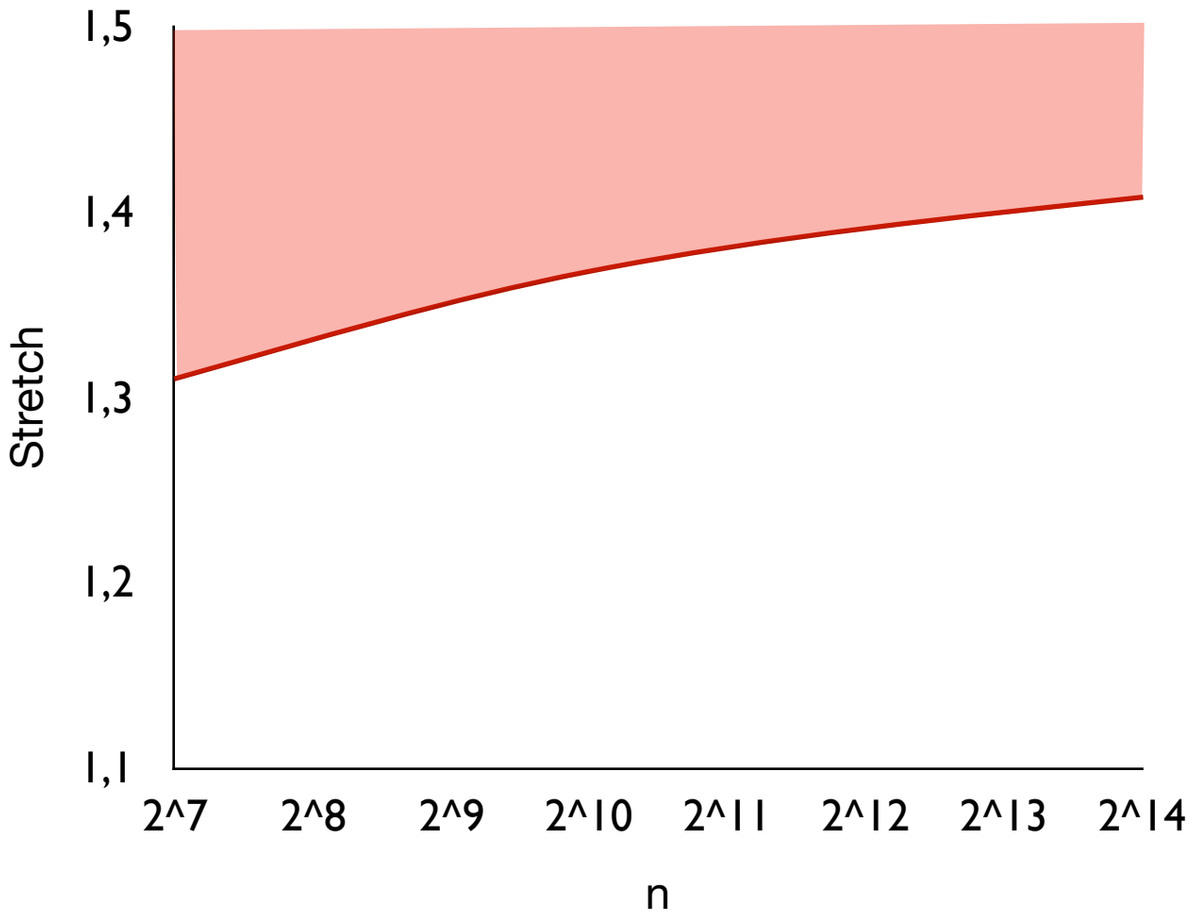


➡ complexity $O(n^{2\omega})$

Gröbner basis approach

Conjectured polynomial attack

For $s \geq f(n)$, the degree of regularity of the Gröbner basis computation is 3 with a degree 2 final resolution



➡ complexity $O(n^{2\omega})$

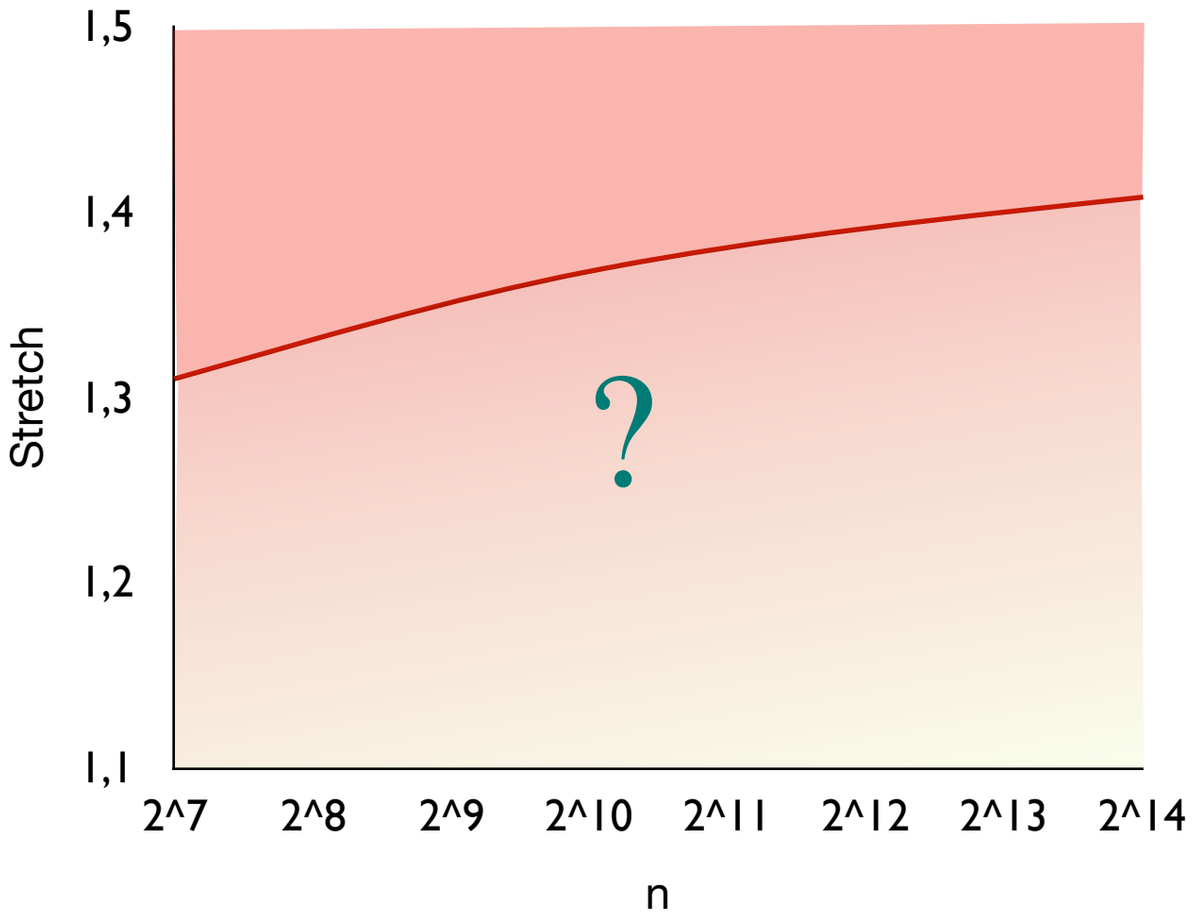
Experiment

- Verified for small n with Faugère's F4

Gröbner basis approach

Conjectured polynomial attack

For $s \geq f(n)$, the degree of regularity of the Gröbner basis computation is 3 with a degree 2 final resolution

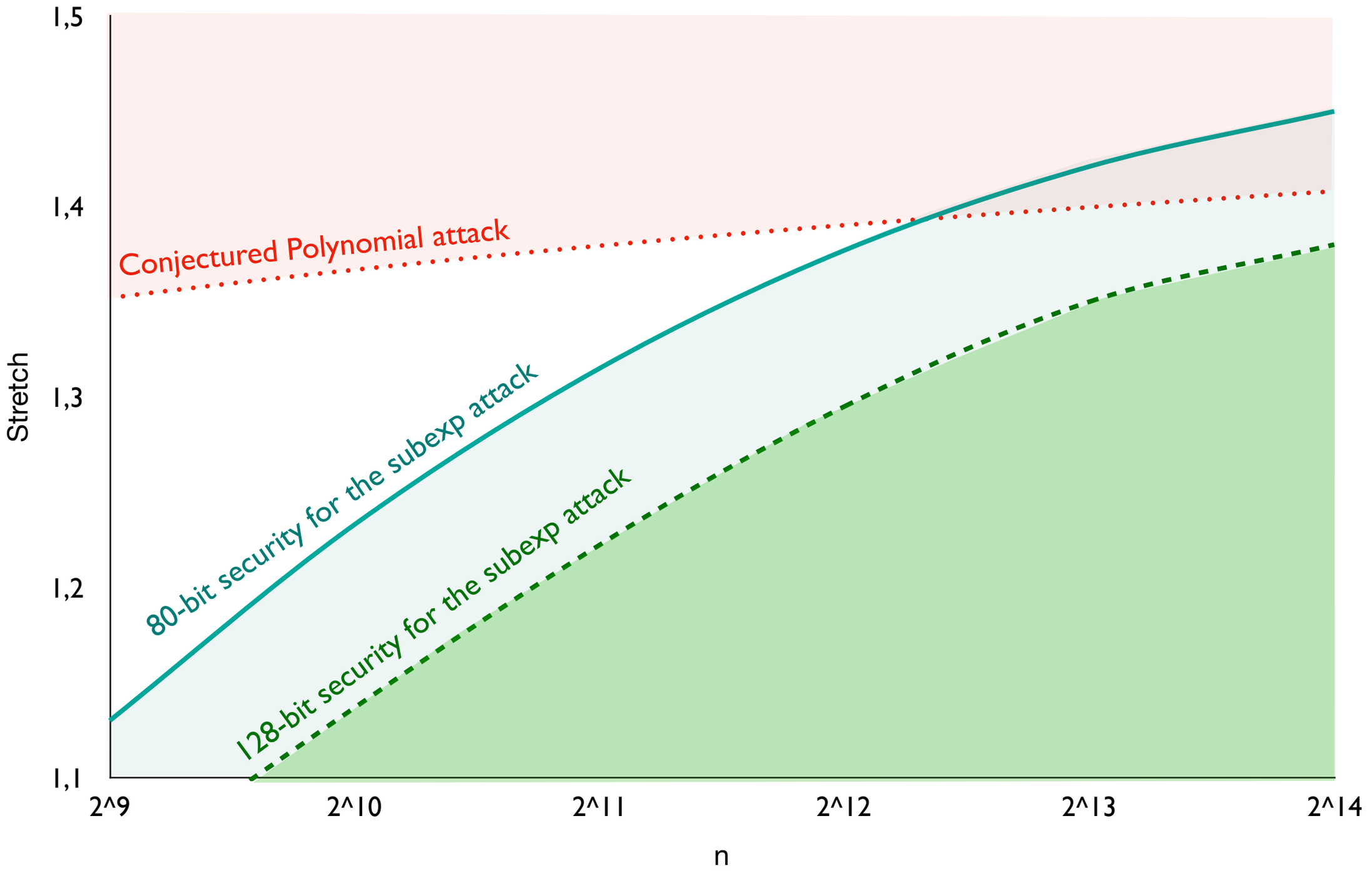


➡ complexity $O(n^{2\omega})$

Experiment

- Verified for small n with Faugère's F4
- Included in the vulnerable parameters

All results


1,5
1,4
1,3
1,2
1,1
Stretch
Conjectured Polynomial attack
80-bit security for the subexp attack
128-bit security for the subexp attack
2^9
2^10
2^11
2^12
2^13
2^14
n

Other contribution

- Our guess and determine attack can be generalized to other predicates:

$$XOR_l MAJ_k(\mathbf{x}) = XOR(x_1, \ldots, x_l) + MAJ(x_{l+1}, \ldots, x_k)$$

XorMaj predicate

Applebaum, Lovett STOC 2016

Other contribution

- Our guess and determine attack can be generalized to other predicates:

$$XOR_l MAJ_k(\mathbf{x}) = XOR(x_1, \ldots, x_l) + MAJ(x_{l+1}, \ldots, x_k)$$

XorMaj predicate

Applebaum, Lovett STOC 2016

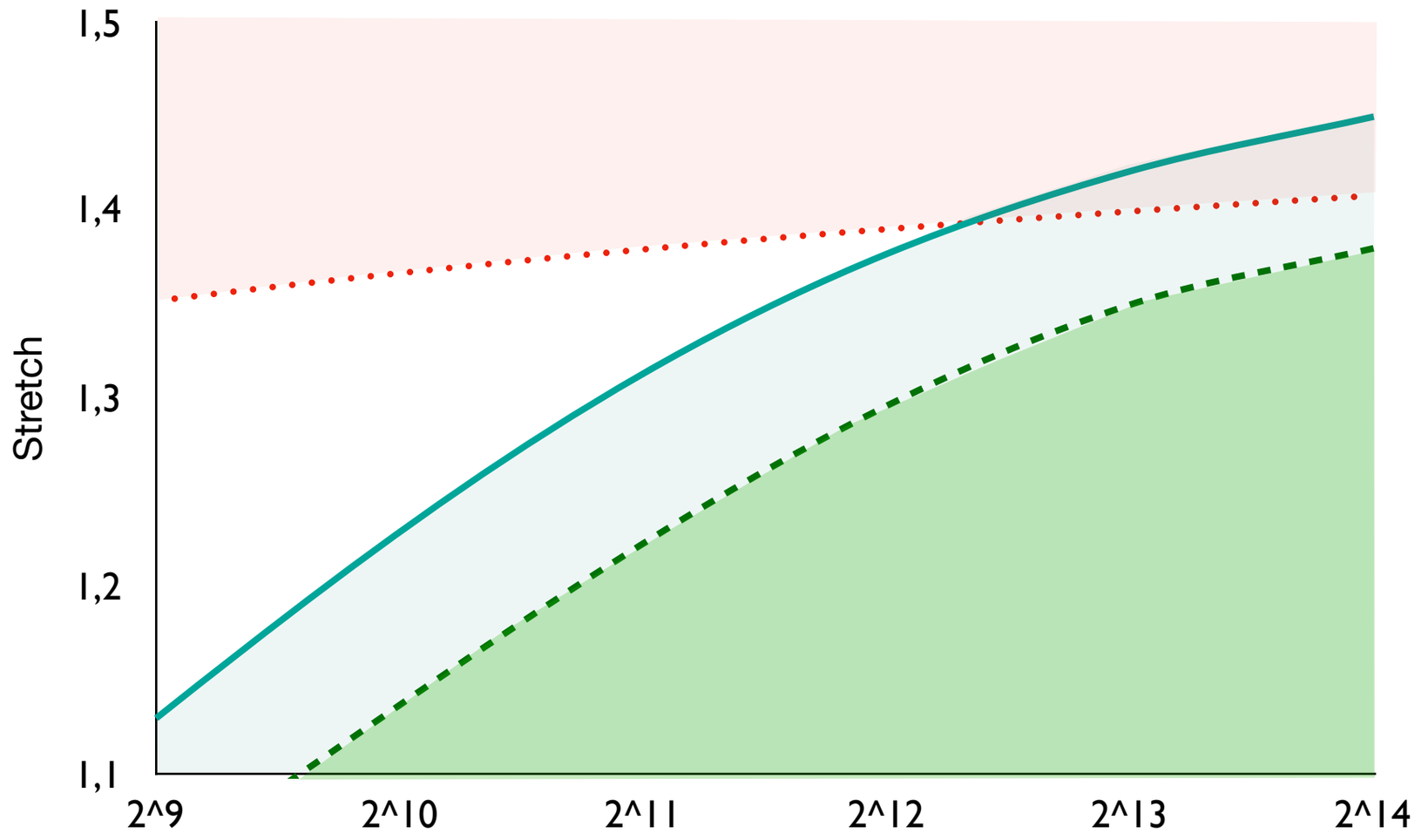
➡ Another approach: The set of guesses is not fixed, and all the guesses are assigned to (0,0,…0) or (1,1,…1)

Total complexity $O\left(n^{\omega} 2^{n\left(1-\frac{s-1}{\left\lceil \frac{k}{2} \right\rceil + 1}\right)}\right)$

Conclusion and open questions

Concrete security of Goldreich PRG with predicate P5 and XorMaj predicates

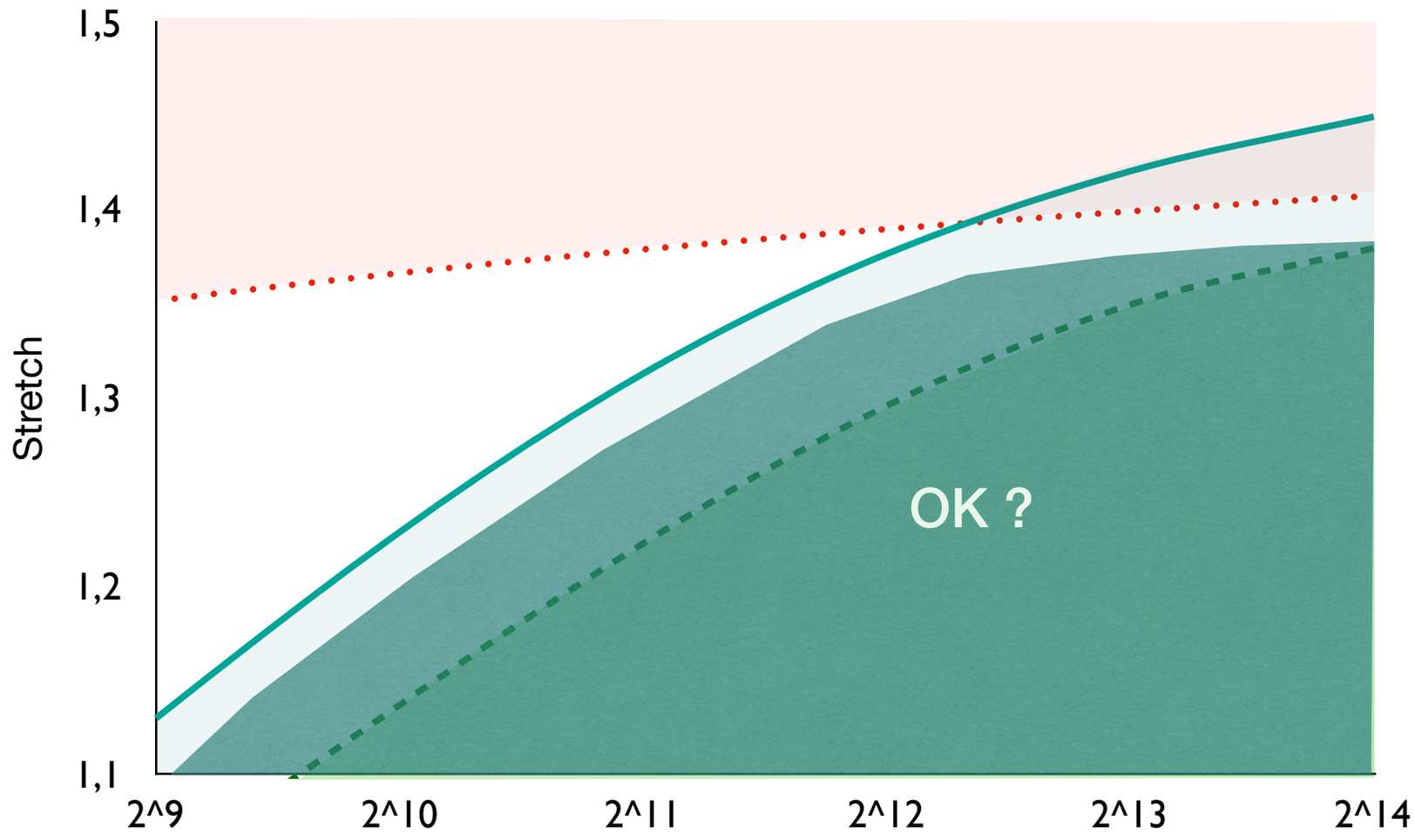
➡ Can we improve the security bounds for P5?



Conclusion and open questions

Concrete security of Goldreich PRG with predicate P5 and XorMaj predicates

➡ Can we improve the security bounds for P5?



Conclusion and open questions

Concrete security of Goldreich PRG with predicate P5 and XorMaj predicates

➡ Can we improve the security bounds for P5?
for other predicates ?

On other predicates, the inequivalence between the guesses must be taken into account

$x_0 + x_1x_2x_3x_4$ → $x_1 = 0$ Linear equation

$x_0 + x_1x_2x_3x_4$ → $x_1 = 1$ Degree 3 equation

Conclusion and open questions

Eprint: https://eprint.iacr.org/2018/1162

Codes: https://github.com/LuMopY/SecurityGoldreichPRG

Conclusion and open questions

Eprint: https://eprint.iacr.org/2018/1162

Codes: https://github.com/LuMopY/SecurityGoldreichPRG

Thank you for your attention