NIST Beacon Architecture.
The Beacon will...

- Broadcast full-entropy bit-strings
- Broadcast blocks of 512 bits per minute
- Sign and time-stamp each block
- Link the sequence of blocks with a secure hash
Database Schema

- Version
- Frequency
- Timestamp
- Random Value
- Previous Hash Value
- Error Code
- Signature
- Current Hash Value
Many forms of human interaction have moved from the meeting table to the Internet.
• Many forms of human interaction have moved from the meeting table to the Internet.

• At a meeting table, six people can roll a die to decide fairly who gets to speak first.
• Many forms of human interaction have moved from the meeting table to the Internet.

• At a meeting table, six people can roll a die to decide fairly who gets to speak first.

• Who rolls the die at a virtual meeting room?
Many forms of human interaction have moved from the meeting table to the Internet.

At a meeting table, six people can roll a die to decide fairly who gets to speak first.

Who rolls the die at a virtual meeting room?

Cryptographers solved this problem in the early 80’s, but the solutions are costly in several ways.
Many forms of human interaction have moved from the meeting table to the Internet.

At a meeting table, six people can roll a die to decide fairly who gets to speak first.

Who rolls the die at a virtual meeting room?

Cryptographers solved this problem in the early 80’s, but the solutions are costly in several ways.

New solution: use a trusted public source of randomness.
From abstraction to real applications.

- Simulating the die and meeting room is a cryptographic primitive.
From abstraction to real applications.

- Simulating the die and meeting room is a cryptographic primitive.
- A practical solution to this primitive is a powerful tool in solving a large class of problems related to transactions in the digital era.
From abstraction to real applications.

- Simulating the die and meeting room is a cryptographic primitive.
- A practical solution to this primitive is a powerful tool in solving a large class of problems related to transactions in the digital era.
- Some examples:
  - Voting.
  - Contract signing (I’ll commit my signature only if you commit yours).
  - Sealed-bid auctions.
  - Many more ...
From abstraction to real applications.

In Tim Polk’s words,

“the Beacon puts us back in the meeting room.”
Beyond simulating the meeting room

New functionalities allow new capabilities ...
Beyond simulating the meeting room

New functionalities allow new capabilities …

enhancing trust, transparency, fairness, privacy, etc. in digital commerce and digital government.
Two Example Applications

- Post-Election Auditing.
- Selection of Qualified Volunteers.
• Texas state law requires post election auditing of “One percent of the election precincts, or in three precincts, whichever is greater.”

• Predictable precinct selection could enable fraud.

• Selection of precincts could skew results.
Selecting Precincts For Auditing

"select first NIST Beacon output after polls close"

seed

Pseudorandom deterministic selection algorithm generates number in range

repeat until sufficient candidates have been selected

Selected precincts
IETF Nominating Committee Selection Process (RFCs 3777 and 3797)

- A pool of qualified volunteers is announced.
- The exact algorithm to be used, including the public future sources of randomness, is made public.
- Once the pre-specified sources of randomness are available, those values plus a summary of the execution of the algorithm for selection are announced.
  - Anyone in the IETF can verify that the correct randomness source values were used and the algorithm was properly executed.
Implementing the IETF Process with the NIST Randomness Beacon

“first NIST beacon output for July 7, 2012”

seed

Pseudorandom deterministic
selection algorithm generates
number in range

repeat until
sufficient
candidates
have been
selected

outputs

1. Alexey
2. Beatrice
3. Joss
4. Pat
5. Russ
6. Sandy
7. Yvonne
Identity a la NSTIC

- A collection of encoded attributes about myself on a portable token.
Identity a la NSTIC

- A collection of encoded attributes about myself on a portable token.
- **Selective disclosure** allows me to reveal only whatever information is necessary to complete a transaction.
Identity a la NSTIC

- A collection of encoded attributes about myself on a portable token.

- **Selective disclosure** allows me to reveal only whatever information is necessary to complete a transaction.

- “I am young enough to join this online forum”
Identity a la NSTIC

- A collection of encoded attributes about myself on a portable token.

- **Selective disclosure** allows me to reveal only whatever information is necessary to complete a transaction.

- “I am young enough to join this online forum”

- “I have a valid prescription for this pain medication” (I might not want to disclose whether the prescription was issued by an oncologist or by an orthopaedic doctor).
Identity a la NSTIC

- A collection of encoded attributes about myself on a portable token.
- Selective disclosure allows me to reveal only whatever information is necessary to complete a transaction.
- “I am young enough to join this online forum”
- “I have a valid prescription for this pain medication” (I might not want to disclose whether the prescription was issued by an oncologist or by an orthopaedic doctor).

The NIST Beacon could make selective disclosure simpler, cheaper, faster.
$T^3_2(x,y,z) = xy + xz + yz$
$T^3_2(x,y,z) = xy + xz + yz$
Majority of three

\[ T^3_2(x, y, z) = xy + xz + yz \]
The problem is to verify these

\[ u = XY \]
Majority of three

\[ T^3_2(x,y,z) = xy + xz + yz \]

too many multiplications
Majority of three

\[ T^3_2(x, y, z) = xy + xz + yz \]

much better
Threshold Functions

What about $T_k^n$?
Threshold Functions

What about $T_k^n$?

\[ T_3^5 = x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + x_1x_3x_5 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5 \]
Threshold Functions

What about $T_k^n$?

$$T_3^5 = \ x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + x_1x_3x_5 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4 + x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + x_2x_3x_4x_5$$

It turns out only 3 multiplications are needed.
Future Plans

• Enhance user interface with REST design.
• Migrate database and web services to NIST public network.
• Increase number and diversity of randomness sources.
• Collaborate with PML to integrate quantum noise sources
  • Two phase approach; PML leads are Josh Bienfang and Sae Woo Nam
Future Architecture.