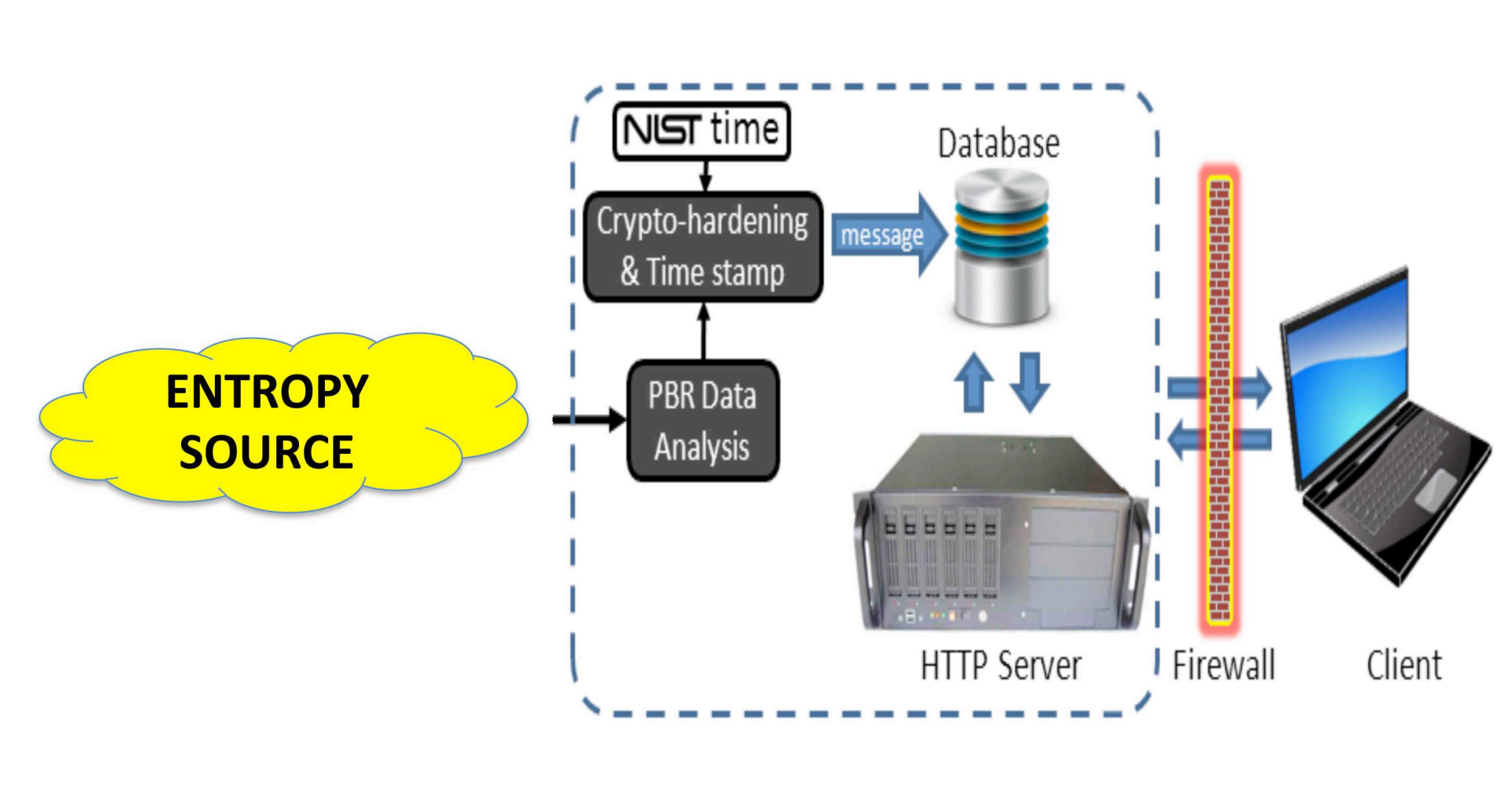
NIST Beacon

Computer Security Division

May 2012

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

Database Snapshot

Microsoft SQL Server Management Studio — 129.6.52.171

File Edit View Debug Query Designer Tools Window Community Help

New Query | Change Type

Object Explorer

Connect

- Databases
  - System Databases
  - RABIN_BEACON
    - Database Diagrams
    - Tables
      - System Tables
      - dbo.BeaconData
        - Columns
          - id (PK, int, not null)
          - version (varchar(32),
          - frequency (int, not n
          - tstamp (bigint, not r
          - random_value (varch
          - previous_hash_value
          - error_code (int, not r
          - signature_value (var
          - current_hash_value (
        - Keys
        - Constraints
        - Triggers
        - Indexes
        - Statistics
    - Views
    - Synonyms
    - Programmability
    - Service Broker
    - Storage
    - Security
  - Security
  - Server Objects

BEACON\SQLEXPR... dbo.BeaconData | Object Explorer Details

id	version	frequency	tstamp	random_value	previous_hash_value	error_code	signature_value	current_hash_value
197	Version 0.1	60	1323186391	CC1AE0A9699FDA6EC...	00000000000000000000...	1	A91B0A1097CA20F25...	E8A4A96A1BBC3BDCAB4EA...
198	Version 0.1	60	1323186451	3417BB48D6A46C41A2...	E8A4A96A1BBC3BDCAB4E...	0	4BDF8DE402A9E8A8F...	8605032EDD8EC1CB9157D...
199	Version 0.1	60	1323186511	145219FF4764F6EB0EB...	8605032EDD8EC1CB9157...	0	39550B16F34807046...	42AD6198EE566D2027DFD...
200	Version 0.1	60	1323186571	89D5FB0B3F6FF3E470...	42AD6198EE566D2027DF...	0	C49746D292D597AC...	15E9FB3DCF5EEC5EBED45...
201	Version 0.1	60	1323186631	BC20B6397D10BDFA57...	15E9FB3DCF5EEC5EBED4...	0	C922DD737D3F845B1...	E768D6C35BA29637F94D36...
202	Version 0.1	60	1323186691	4724E2A7895DDD7288...	E768D6C35BA29637F94D...	0	940EC57B2262620D1...	0C40298746ED8FE488CB4B...
203	Version 0.1	60	1323186751	43C04716C8E7F62529...	0C40298746ED8FE488CB...	0	67BF3ECC089088E22...	0FA1B3BD580186B3CB5DC...
204	Version 0.1	60	1323186811	AF6701DD44AA6BACD...	0FA1B3BD580186B3CB5D...	0	9D76FC7CBA71C75B...	F518AF3EA0712565D51363...
205	Version 0.1	60	1323186871	565851D7C4CF4230CE...	F518AF3EA0712565D513...	0	10C7D085EAFD79927...	92DAF20BEDCFF2B8B84BB3...
206	Version 0.1	60	1323186931	0F1613E6C1DCC67D95...	92DAF20BEDCFF2B8B84B...	0	4F4EF91C529031A59...	F7B2B8443935487F182396...
207	Version 0.1	60	1323186991	07AE3E171FE174F777...	F7B2B8443935487F18239...	0	6A92379AE0AE40180...	62F664DE7A21DBDB703914...
208	Version 0.1	60	1323187051	8C41CAB976F287A553...	62F664DE7A21DBDB7039...	0	5CD4FB8B832888721...	ACB9E0A078A5D35B9FAD7...
209	Version 0.1	60	1323187111	92565B4EE360F6A79E...	ACB9E0A078A5D35B9FAD...	0	B96149B66D9D38FED...	875232220150AC72A04D40...
210	Version 0.1	60	1323187171	E6FEB4F2894830C1A2...	875232220150AC72A04D...	0	78565ACEDEBC9C2F...	FB47D32C95DC4C01284B9...
211	Version 0.1	60	1323187320	51DD0D82216EC5E1FD...	FB47D32C95DC4C01284B...	2	5EE4ACD518B1B737E...	7F78B75C2692675E11BC91...
212	Version 0.1	60	1323187380	603BE0A6C1C8155D69...	7F78B75C2692675E11BC9...	0	95A4063EFA3F8445A...	C3D3A41D43ACC43FFB850...
213	Version 0.1	60	1323187440	BDA22B6F4A5363282A...	C3D3A41D43ACC43FFB85...	0	6AACABBA38BE8264...	2AEEE8CCD2B53C63F157C...
214	Version 0.1	60	1323187500	849D3F72E8A4DF2746...	2AEEE8CCD2B53C63F157...	0	8763FB8B8DD62680F...	A5036103B1E04E31481F85...
215	Version 0.1	60	1323187560	68917A677DD6C469C4...	A5036103B1E04E31481F8...	0	12248ADDB7DC33B8...	04C107A184ACE193F266D...
216	Version 0.1	60	1323187620	5AB83FBC9F85D3FCD4...	04C107A184ACE193F266...	0	07F08A0D1B8EE9047...	3CCE55572A32C134F5CDC...
217	Version 0.1	60	1323187680	A4A4735CB4C9DD2380...	3CCE55572A32C134F5CD...	0	7A83AA3595C54EF1...	3A0EF597E0B573E8CD56B5...
218	Version 0.1	60	1323187740	95F817B3486C597700...	3A0EF597E0B573E8CD56...	0	AD97DBB782134908C...	7C8F119A11E0D96A35D8E...
219	Version 0.1	60	1323187800	1E5A03A240A713E39E...	7C8F119A11E0D96A35D8...	0	115BA8625654F2CCB...	6992739C4A8C20E014105E...
220	Version 0.1	60	1323187860	3AA7186EBDA8FE8CBF...	6992739C4A8C20E01410...	0	97A534BA8E56AAB18...	D117C8CFB8741513DA891...
221	Version 0.1	60	1323187920	4A457BCB513E723BF6...	D117C8CFB8741513DA89...	0	A777F1E4EAF2E352E...	2A3560F89FFA369650BAE2...
222	Version 0.1	60	1323187980	2FCF453922A8E3DBB3...	2A3560F89FFA369650BA...	0	600D99936C35E2158...	9534B9B14E203FD4218AF1...

1 of 200 | Cell is Read Only.

Ready

8:20 AM 4/10/2012

What for.

- Many forms of human interaction have moved from the meeting table to the Internet.

What for.

- 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.

What for.

- 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?

What for.

- 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.

What for.

- 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.

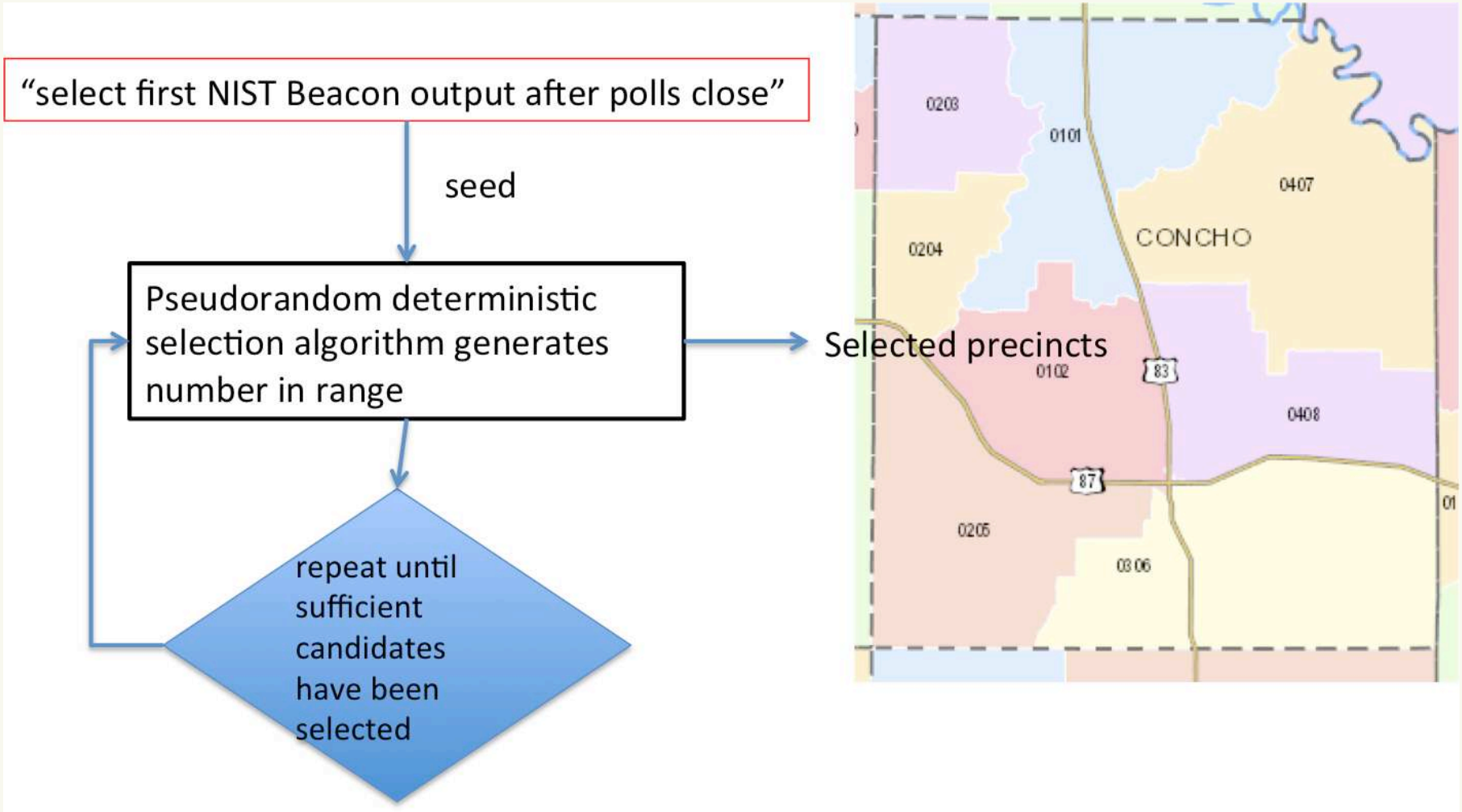
Two Example Applications

- Post-Election Auditing.
- Selection of Qualified Volunteers.

Post-Election Auditing

- 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.

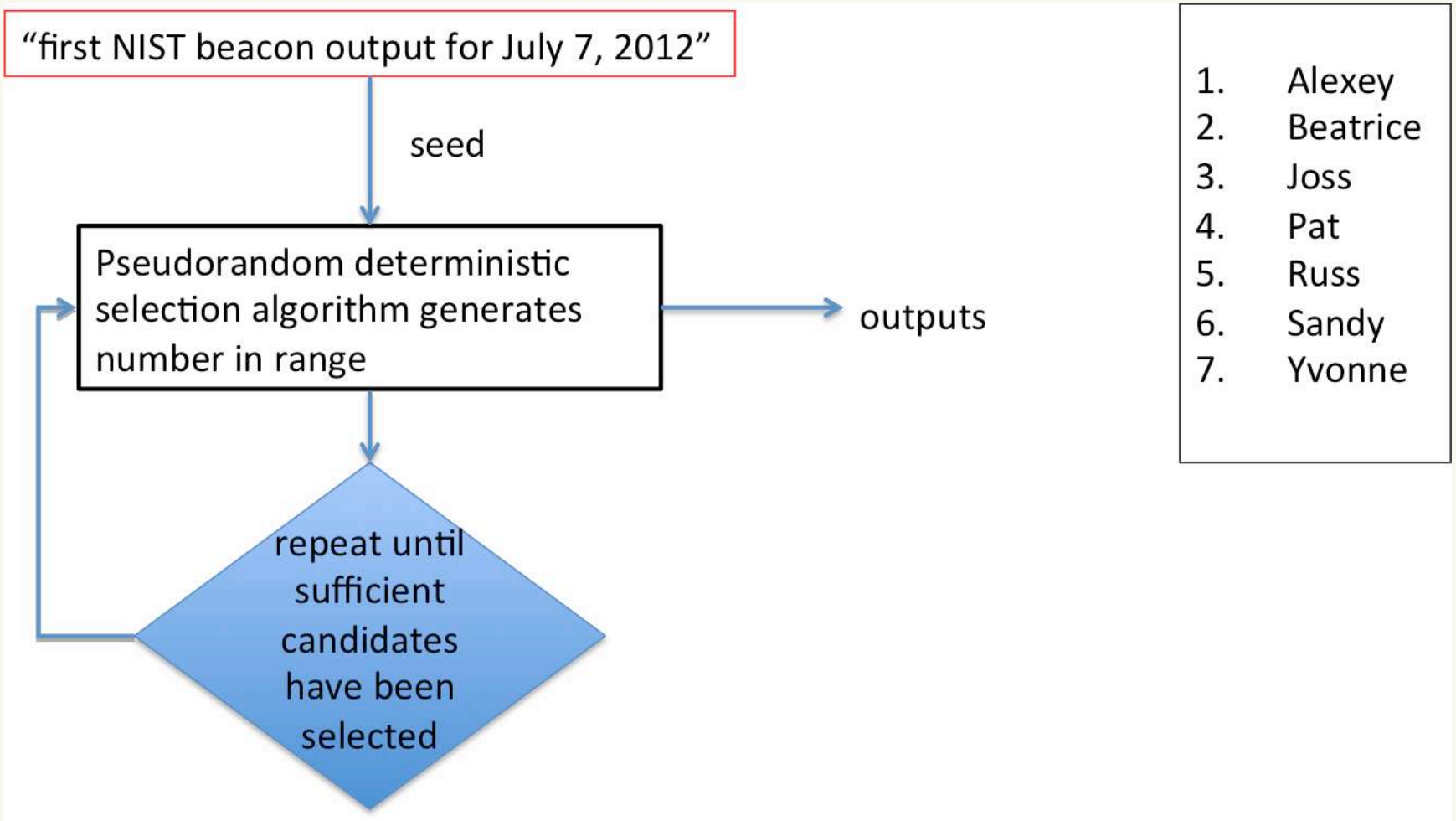
Selecting Precincts For Auditing



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



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

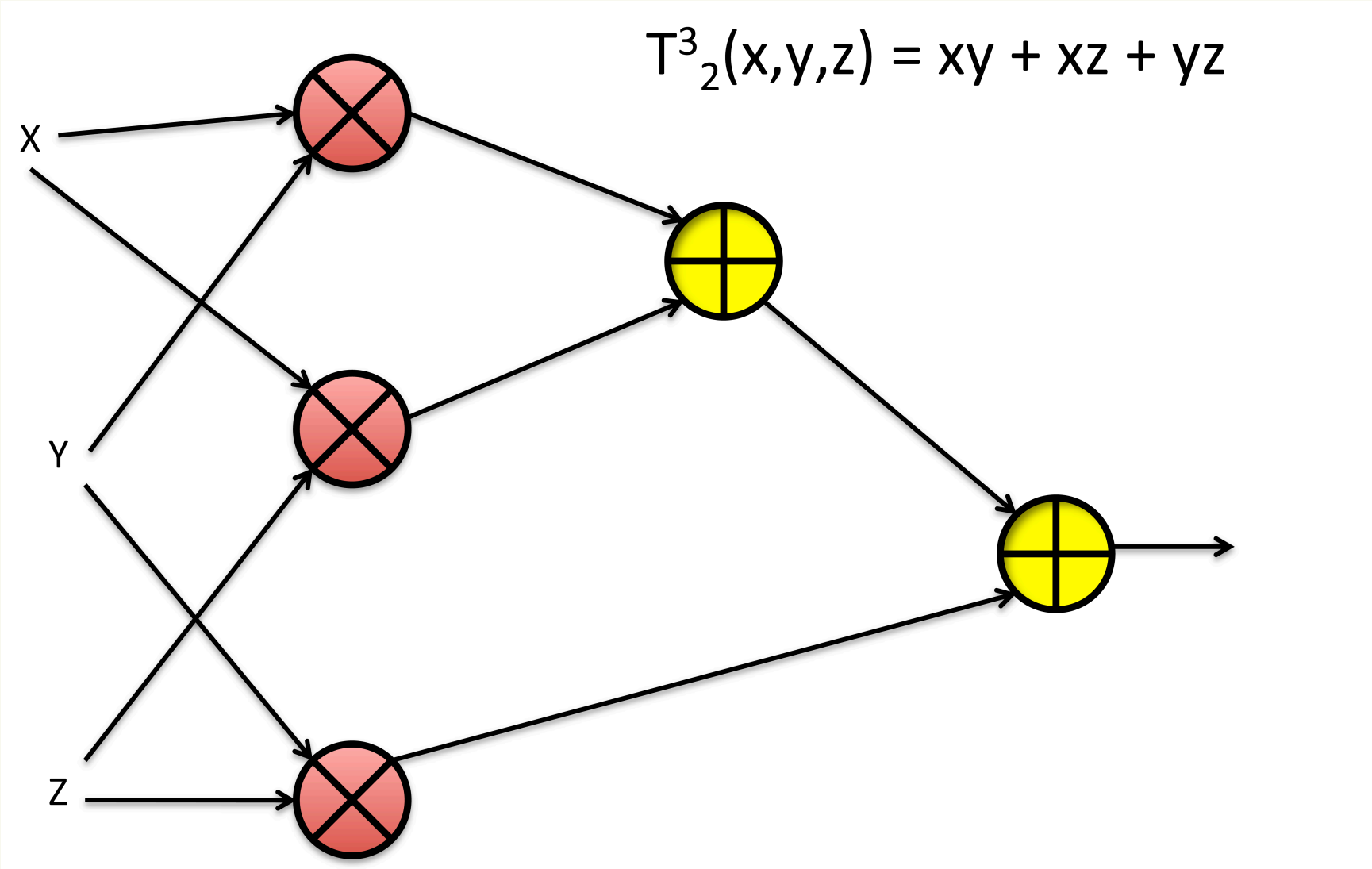
- A collection of encoded attributes about myself on a portable token.
- Selective disclosure allows me to reveal only whatever information is necessary to complete a transaction.
- “I am young enough to join this online forum”
- “I have a valid prescription for this pain medication” (I might not want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

Identity a la NSTIC

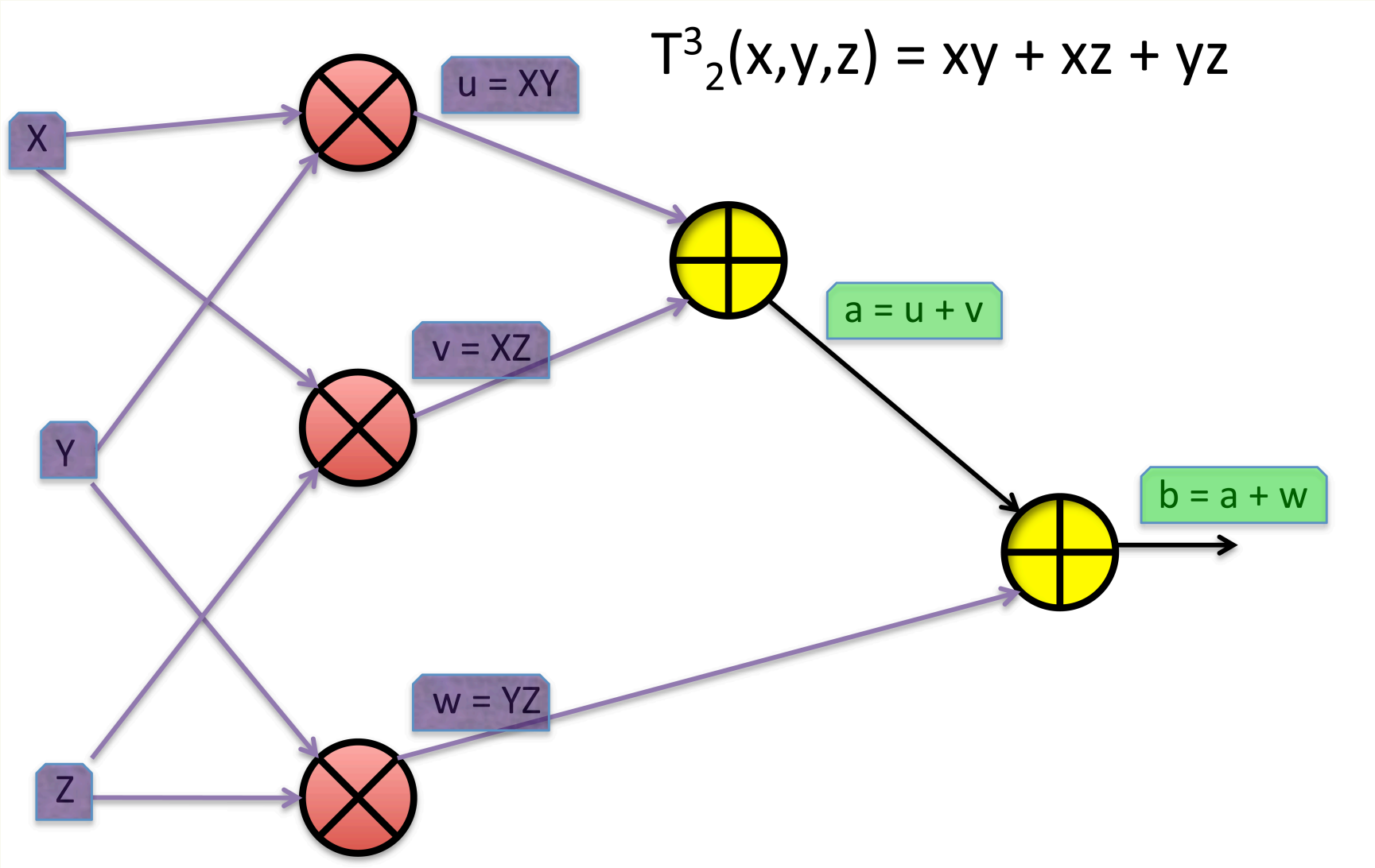
- A collection of encoded attributes about myself on a portable token.
- Selective disclosure allows me to reveal only whatever information is necessary to complete a transaction.
- “I am young enough to join this online forum”
- “I have a valid prescription for this pain medication” (I might not want 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.

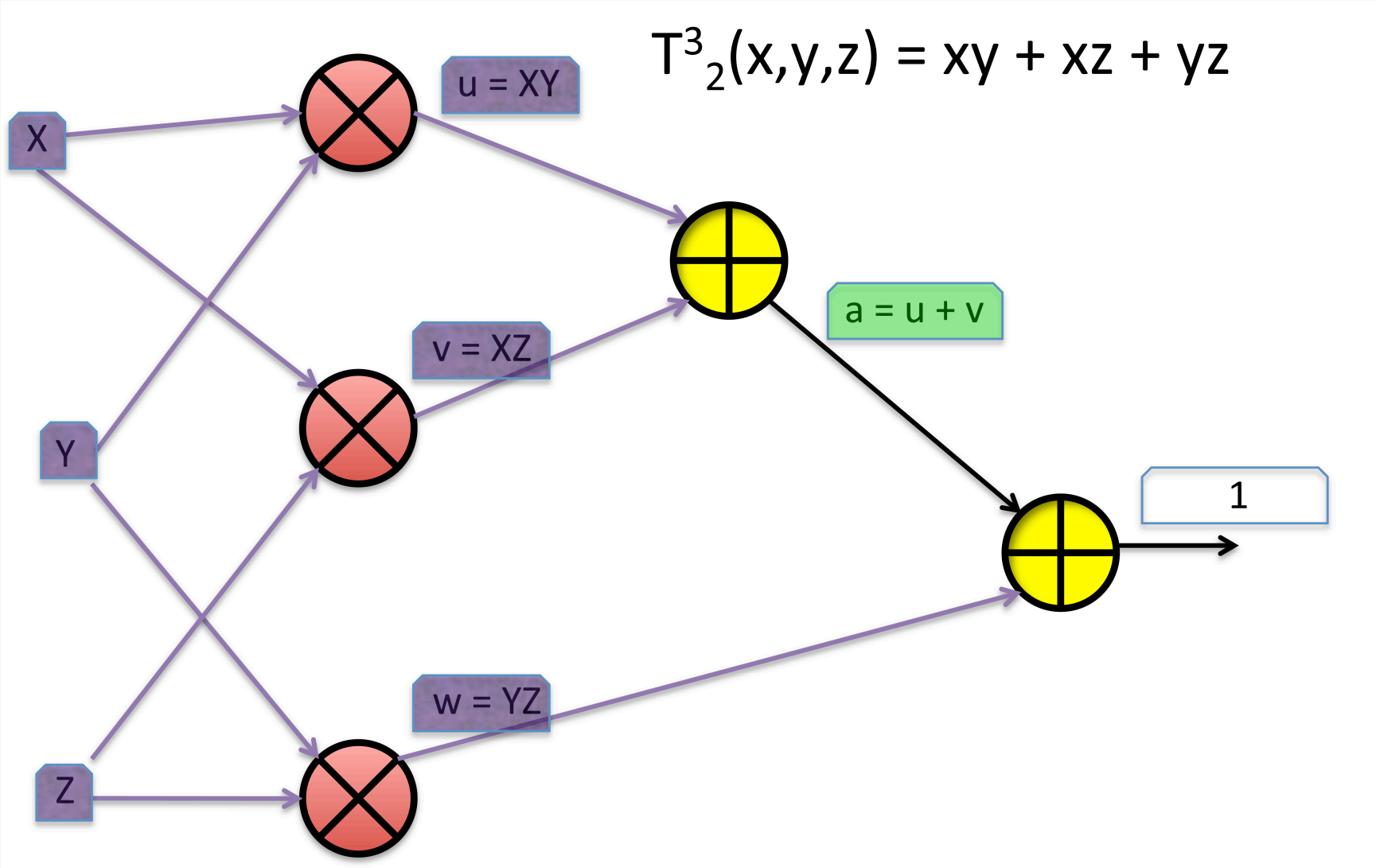
Majority of three



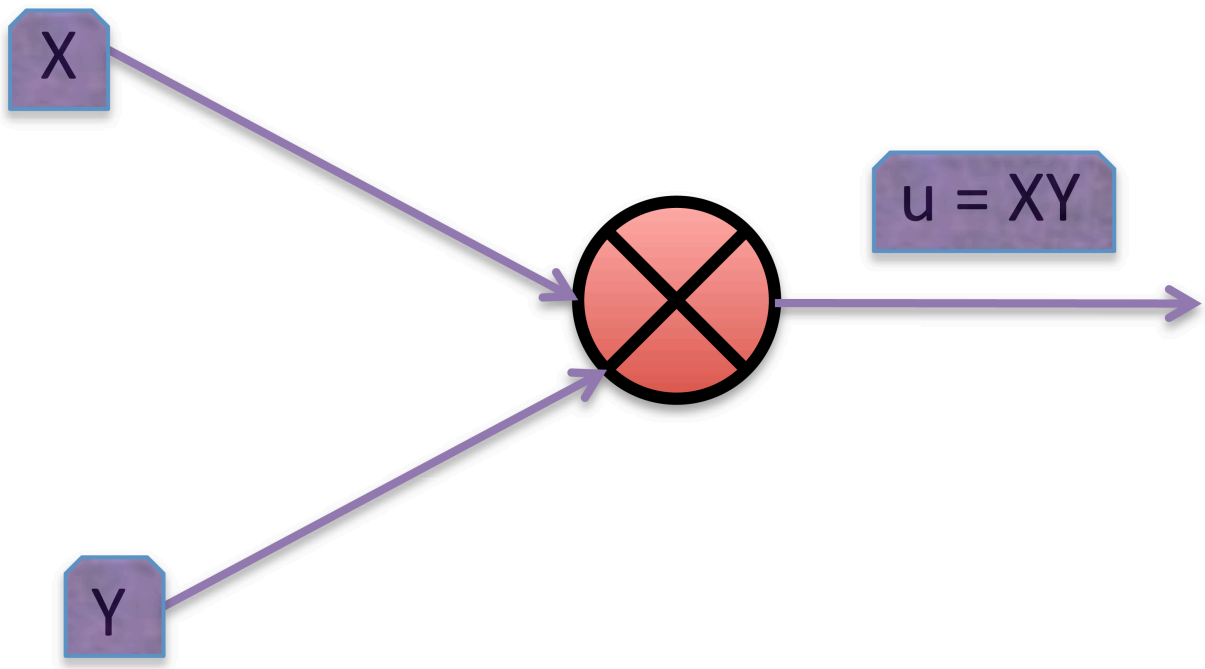
Majority of three



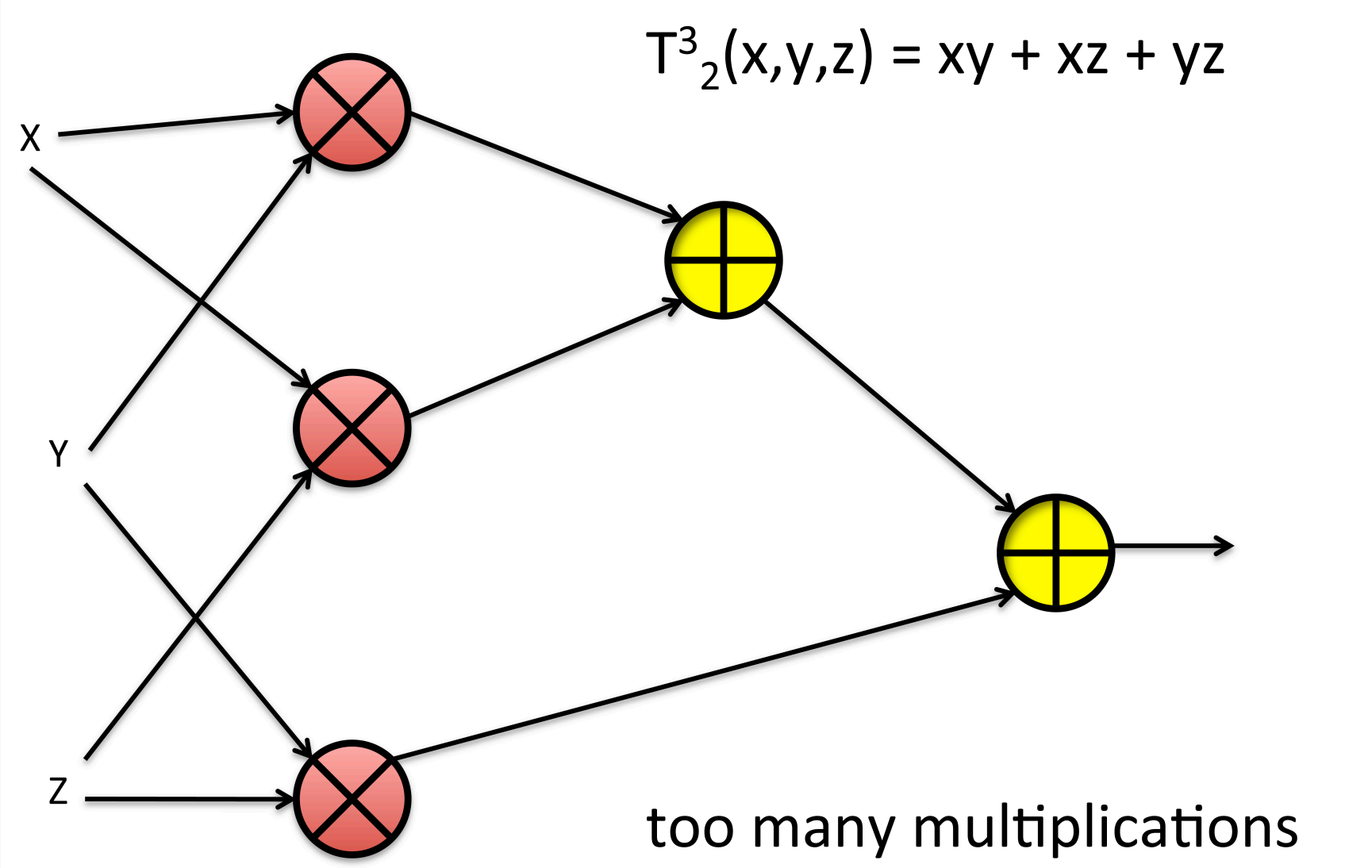
Majority of three



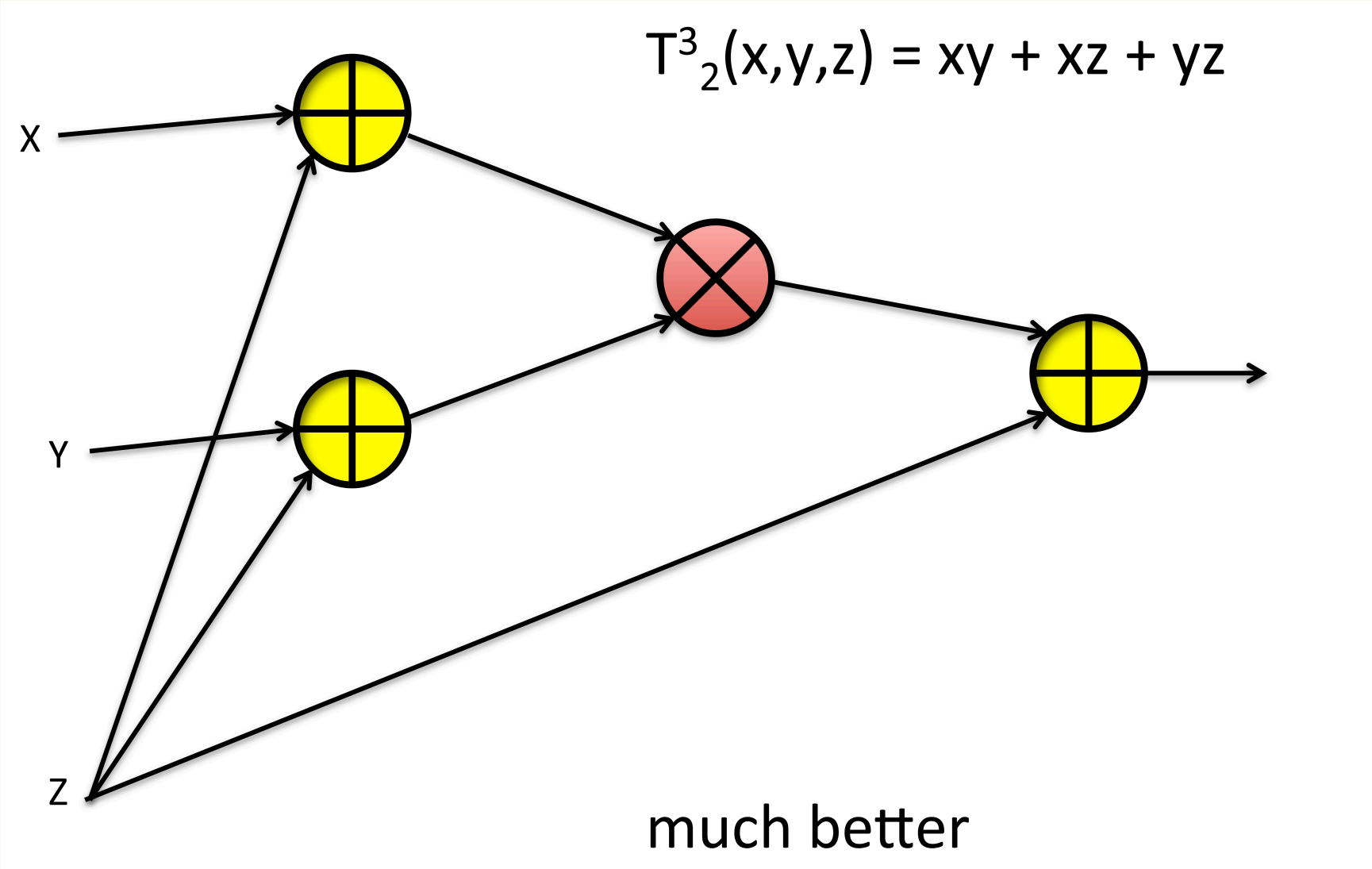
The problem is to verify these



Majority of three



Majority of three



Threshold Functions

What about T_k^n ?

Threshold Functions

What about T_k^n ?

$$
\begin{aligned}
T_3^5 \quad = \quad & x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + \\
& x_1x_3x_5 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + \\
& x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4 + \\
& x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + \\
& x_2x_3x_4x_5
\end{aligned}
$$

Threshold Functions

What about T_k^n ?

$$
\begin{aligned}
T_3^5 \quad = \quad & x_1x_2x_3 + x_1x_2x_4 + x_1x_2x_5 + x_1x_3x_4 + \\
& x_1x_3x_5 + x_1x_4x_5 + x_2x_3x_4 + x_2x_3x_5 + \\
& x_2x_4x_5 + x_3x_4x_5 + x_1x_2x_3x_4 + \\
& x_1x_2x_3x_5 + x_1x_2x_4x_5 + x_1x_3x_4x_5 + \\
& x_2x_3x_4x_5
\end{aligned}
$$

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

NIST Beacon

Future Architecture.