MATHMESH BOF

Phillip Hallam-Baker

10am Monday Collyer

Make computers easy to use by making them more secure

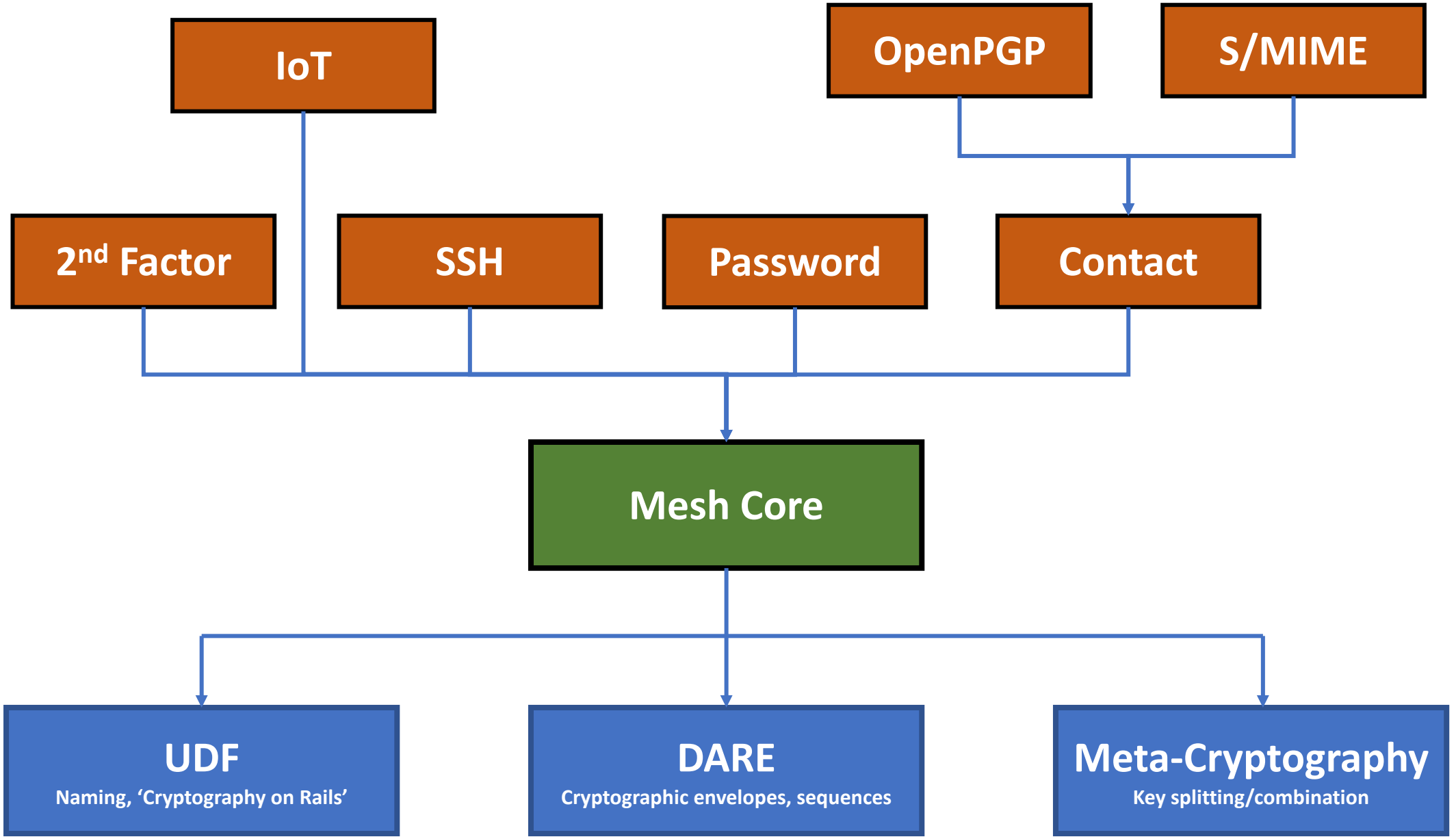
- Cryptographically connect every device Alice owns to each other
  - Alice's personal Mesh
  - Use that framework to authenticate maintenance messages
  - Enable use of strong end-to-end encryption

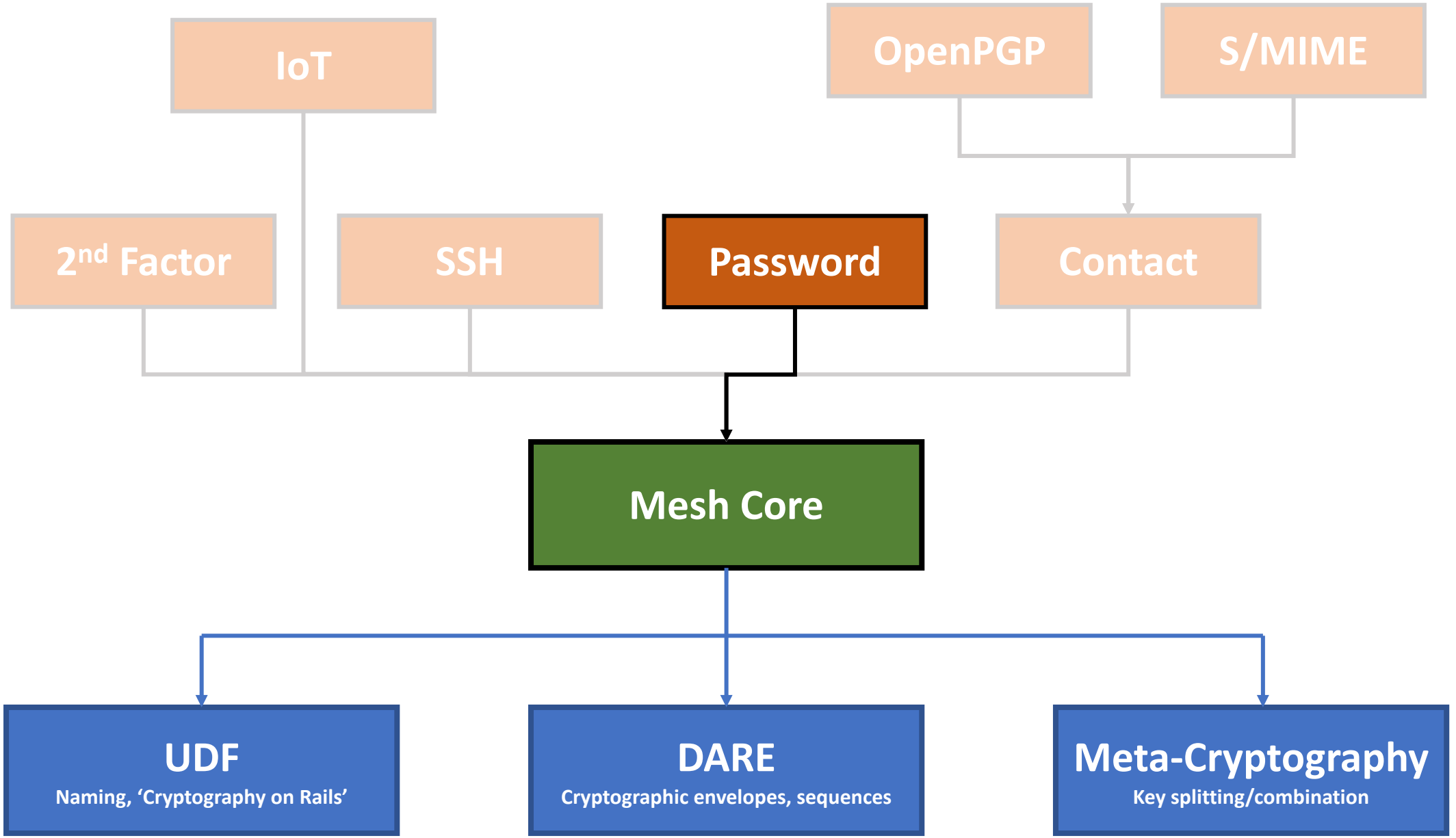
- 3 Core problems
  - Provision private keys to devices
  - Provide the means to obtain and validate public keys
  - Secure data at rest

Security today

- SSH
- OpenPGP, S/MIME
- Signal, Keybase, WhatsApp, etc. etc.
- Anti-virus
- NAT / VPN
- Spam filtering

- Separate products, separate dashboards
  - Security falls between the cracks


IoT
OpenPGP
S/MIME
2nd Factor
SSH
Password
Contact
Mesh Core
UDF
Naming, 'Cryptography on Rails'
DARE
Cryptographic envelopes, sequences
Meta-Cryptography
Key splitting/combination


IoT
OpenPGP
S/MIME
2nd Factor
SSH
Password
Contact
Mesh Core
UDF
Naming, 'Cryptography on Rails'
DARE
Cryptographic envelopes, sequences
Meta-Cryptography
Key splitting/combination

Why choose passwords?

Mesh Password Catalog

- Test application, provides 90% coverage
  - Requires minimal additional code for use
- Immediate value
  - Does not rely on network effect
  - Addresses ‘functional password’ problem
- An open standard for a good password vault
  - Enables use of strong (128 bit WF) passwords
  - **Provides path to replace passwords (public keypair provisioned)**

Alice’s Personal Mesh (Technical view)

- Make Alice her own ultimate root of trust
  - She can delegate trust to a 3rd party
    - Can reclaim her autonomy at any time
  - Alice creates a personal Mesh profile
    - Master Signature Key
      - Never changes
      - Is only used to sign (infrequent) updates to Alice’s Mesh profile
      - May be stored offline
    - Administration keys
      - Used by administration devices to sign device connection assertions

Alice's Personal Mesh (User view)

- Alice installs application on her mobile phone
  - Creates account `alice@example.com`

- Alice can add more devices
  - By scanning a QR code
  - By installing an app and requesting connection to `alice@example.com`
    - New device shows `AA4W-JXKO-TG2S-JSDH-7AYY-BY5Q-UPH4`
    - Admin device shows `AA4W-JXKO-TG2S-JSDH-7AYY-BY5Q-UPH4`
    - They are the same, Alice accepts, device is connected

Connected devices can access shared catalogs

- Every connected device has the same world view
  - Alice can use a personalized vocabulary with voice activated devices
    - “Zen, turn on lights in the yellow room”
    - The term ‘yellow room’ is in Alice’s contacts file, it is personal to her
  - Add/change a task, contact, bookmark, password on one device
    - Every other connected device has access
- Every connected device can authenticate messages as being ‘of Alice’
  - Can establish a single dashboard for her IoT devices

Mesh Components

- Mesh Schema
  - Capabilities similar to SAML/PKIX
  - Uses JSON data model
- Mesh Account
  - Alice has one Mesh but 4 separate accounts (business/personal/restaurant)
  - These accounts belong to Alice
- Mesh Service
  - Synchronization of Catalogs
  - Always available point of contact for messaging

Discuss: Mesh overview

- Web site
  - Mathmesh.com
- YouTube Channel
  - 7 hours of video

- Technology items still to come
  - UDF
  - DARE
  - Meta-Cryptography

UDF

Cryptography on Rails

BASE-32 encoding of cryptographic data

- Content Digest
  - `MB5S-R4AJ-3FBT-7NHO-T26Z-2E6Y-WFH4`
  - `KCM5-7VB6-IJXJ-WKHX-NZQF-OKGZ-EWVN`
- Message Authentication Code
  - `AA4W-JXKO-TG2S-JSDH-7AYY-BY5Q-UPH4`
- Symmetric Encryption Key
  - `EDUL-JOAU-5HCC-F233-F5CT-JX64-3F5Q`
- Public Key Pair
  - `ZAAQ-AWMQ-6Z4O-RRMM-Y72J-CGWI-ZC7L-V5Y`
- Shamir Secret Share
  - `SAQH-4253-OUIQ-QB3Z-FEU5-V3V3-D75X-S`

Cryptography on rails

- All Mesh key-ids are Content-Digest UDFs
  - SHA-2-512 digest of the key
  - No PKIX Path-Math complications

Encrypted QR Code

- udf://example.com/ECXI-SNKI-GDCM-2DCP-WPBG-KNNQ-Z2NJ-WI

- udf://example.com
  - Try DNS Service Discovery SRV/TXT resolution
  - https://example.com/.well-known/mmm-udf/ <UDF (“ECXI-…-WI”)>
    - MB7N-KULZ-C5WW-EOYW-SLTL-JJTU-LKND-SOXY-YHSI-KQE6-Z4FS-YRGE-UVBD-PRPV

- Fetch document, it is encrypted
  - The decryption key is ECXI-SNKI-GDCM-2DCP-WPBG-KNNQ-Z2NJ-WI

For more information

- Web site
  - Mathmesh.com
- YouTube Channel
  - 7 hours of video

DARE

Blockchain in JSON

Data At Rest Envelope

- PKCS#7 for JSON Signature & Encryption (JOSE)
  - Re-uses the same crypto
  - Mesh uses standard Encryption, Signature and Verification
    - Decryption changes
    - Key provisioning changes
  - Uses KDF (<master secret>, <nonce>) to derive
    - IV and Encryption
    - MAC Key (if needed)
    - Signature witness value (to provide plaintext binding)

DARE Sequence

- Append only log format
  - Incremental authentication (Merkle Tree)
    - Can sign head of chain
  - Incremental encryption
    - Can encrypt 100 envelopes under same <master secret>
      - Just use a different nonce
- Can support an archive format
  - (Used as a test mule)

Dare Catalog

- Persistence store based on DARE Sequence
  - A set of cataloged objects with a unique ID
    - Sequence of Add/Update/Delete transactions
  - Objects may be encrypted
    - Can discuss exact encryption boundary offline.

- Synchronize a DARE catalog by synchronizing DARE sequence
  - Mesh Service protocol is very simple
    - Status/Upload/Download

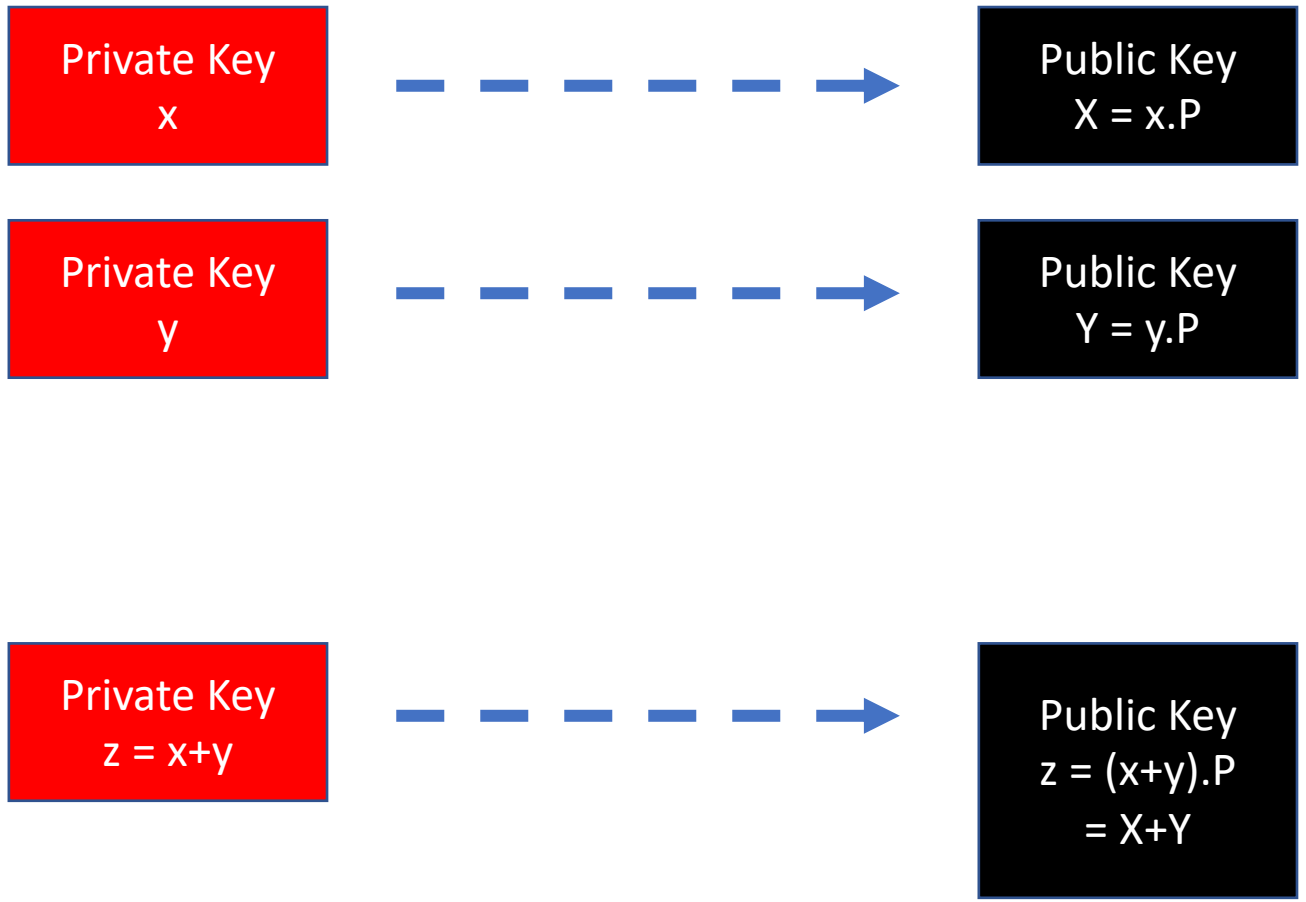
For more information

- Web site
  - Mathmesh.com
- YouTube Channel
  - 7 hours of video

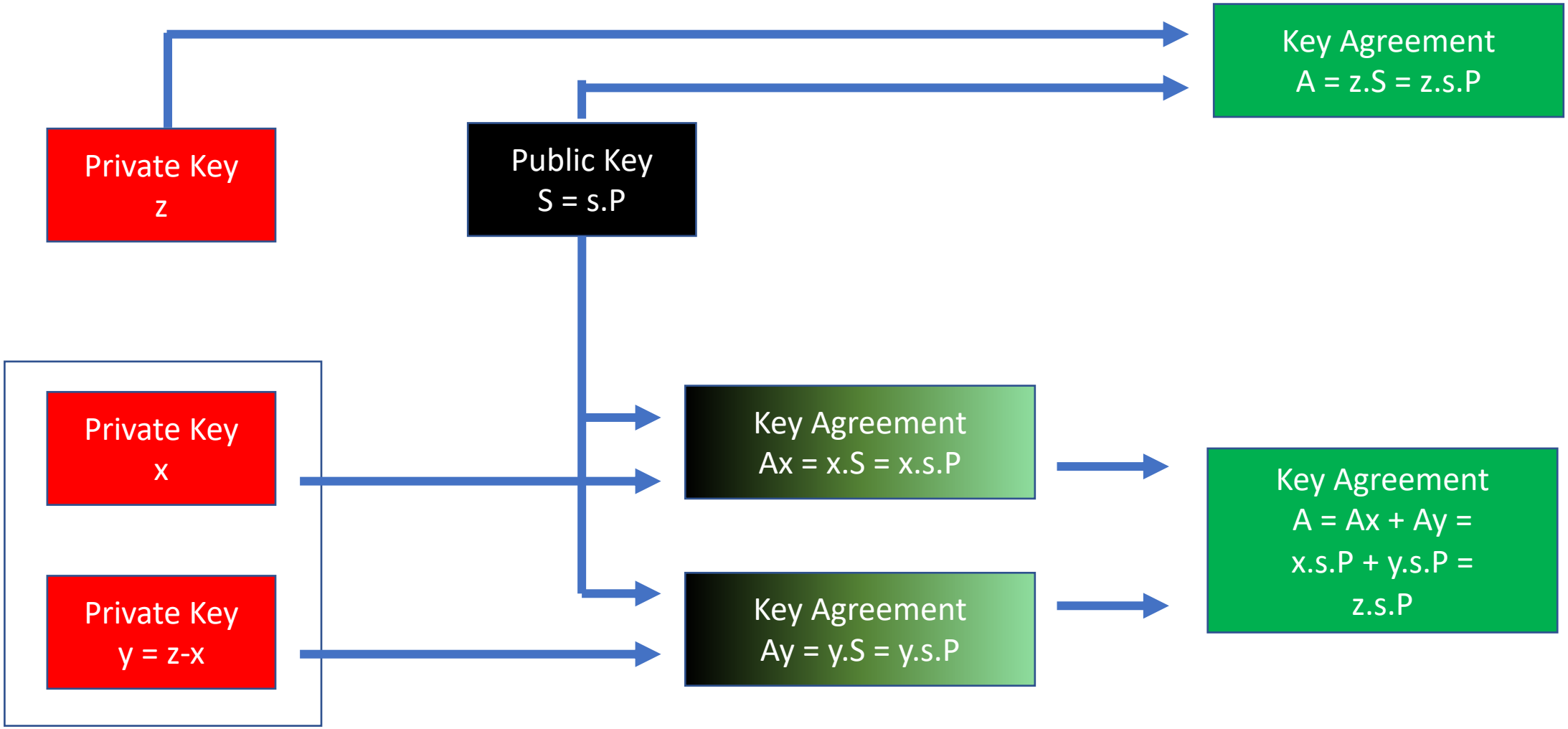
Meta Cryptography

Web 2.0 Rebranding for threshold cryptography etc.

Key Combination

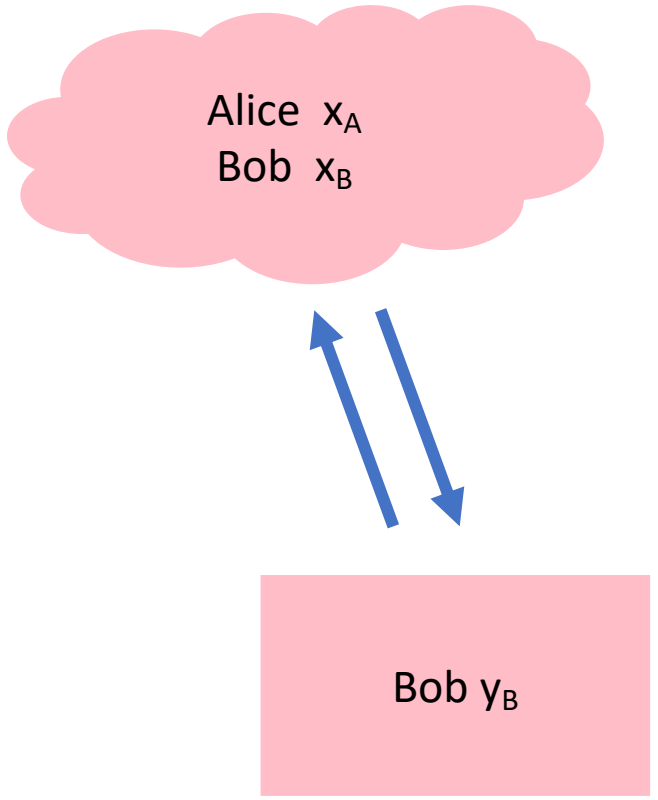


Key Splitting



Snowden-Proof Key Management

- Cloud service can control decryption
  - But cannot decrypt
  - The cloud only knows a random number
    - Can be generated without knowledge of private key



For more information

- Web site
  - Mathmesh.com
- YouTube Channel
  - 7 hours of video