IPSec Present and future

P.V. Ananda Mohan Ph.D.
Fellow IEEE
CDAC, Bangalore

AGENDA

- IPSec Introduction
- Protocols in IPSec
- Attacks on IPSec
- IPSec in post-quantum era
- Conclusion

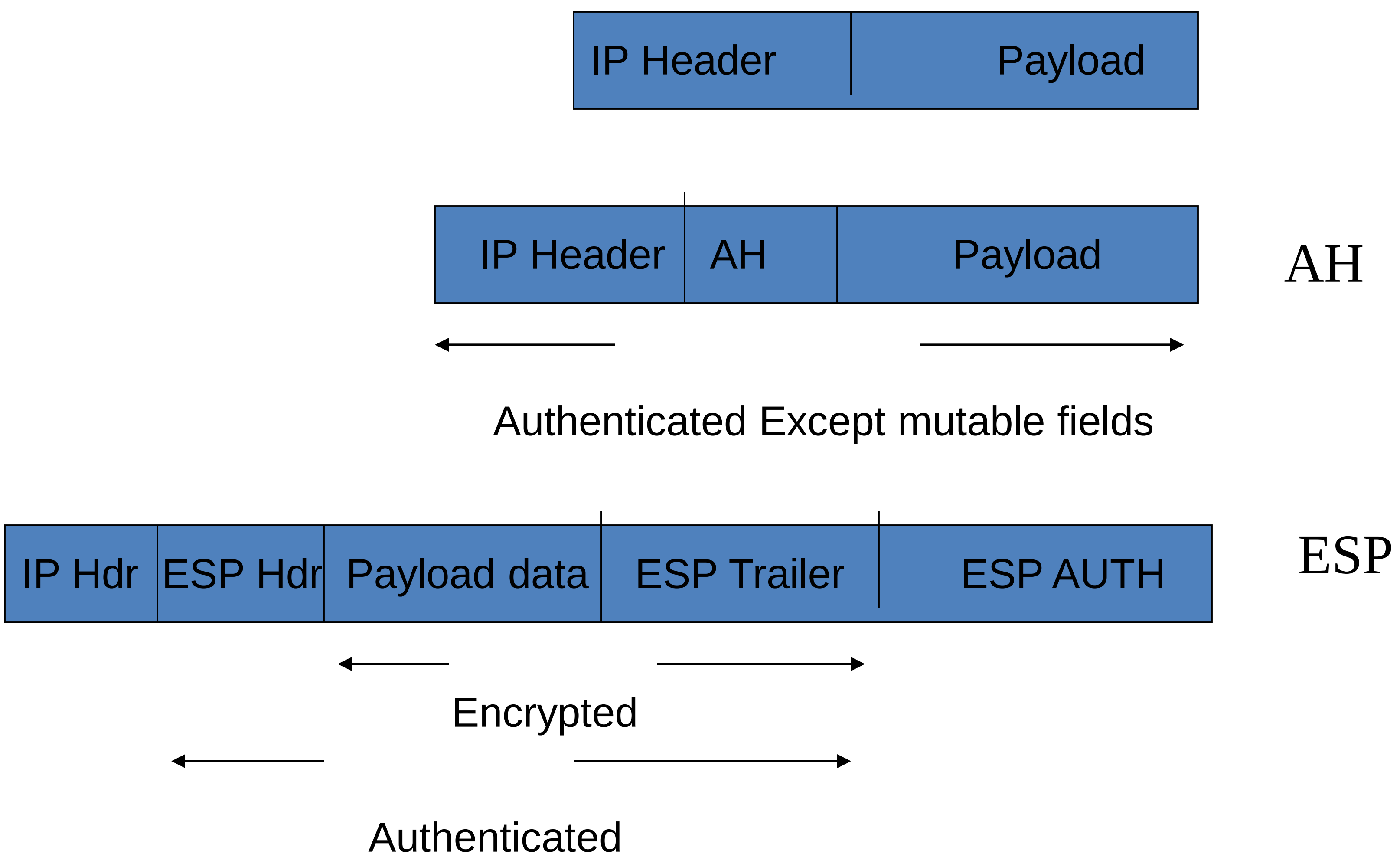
An Internet packet

<table>
<tr><td>VERS</td><td>HLEN</td><td>SERVICE TYPE</td><td colspan="2">TOTAL LENGTH</td></tr>
<tr><td colspan="3">IDENTIFICATION</td><td>FLAGS</td><td>FRAGMENT OFFSET</td></tr>
<tr><td colspan="2">TIME TO LIVE</td><td>PROTOCOL</td><td colspan="2">HEADER CHECKSUM</td></tr>
<tr><td colspan="5">SOURCE IP ADDRESS</td></tr>
<tr><td colspan="5">DESTINATION IP ADDRESS</td></tr>
<tr><td colspan="4">IP OPTIONS IF ANY</td><td>PADDING</td></tr>
<tr><td colspan="5">DATA</td></tr>
</table>

IPsec

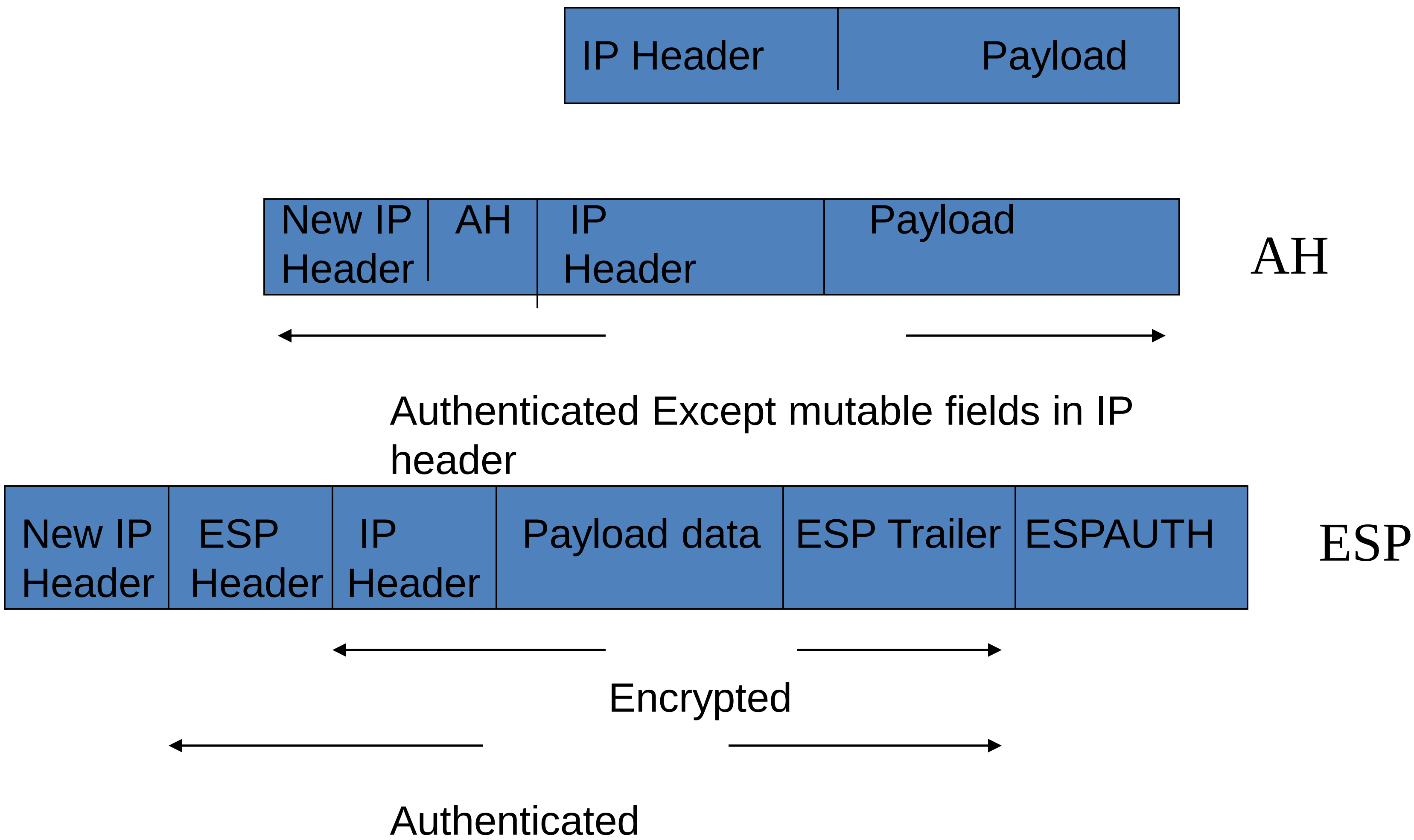
- Provides Security services at the IP layer
- Two mechanisms
- **Authentication Header** provides data integrity, data origin authentication, and protects the payload from replay attacks using sequence number
- **ESP** (encapsulation Security Payload) provides confidentiality, data origin authentication.
- Relationships between devices are called SA (**security associations**)
- Policy controlled by Security Policy Database (SPD)
- Key Management scheme is IKE (**Internet Key exchange**)
- ISAKMP (I**nternet Security association key management protocol**) for authentication and key exchange)

IP Sec in Transport Mode



- AUTH is obtained by HMAC and MSB 96 bits are chosen. HMAC-MD5-96 or HMAC-SHA1-96

IP Sec in Tunnel Mode

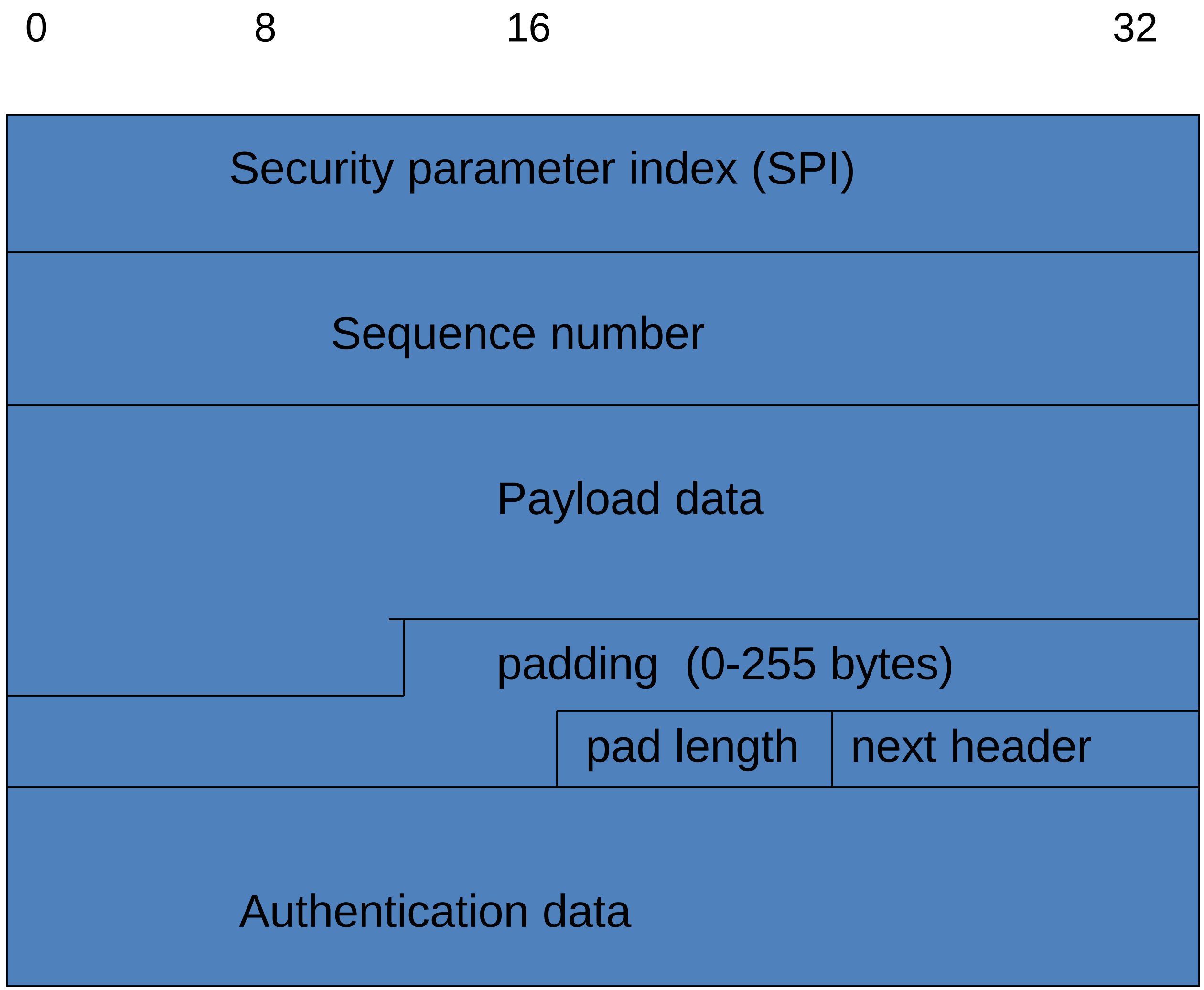


AH

0	8	16	32
Next header	Payload length	Reserved	
Security parameter index (SPI)			
Sequence number			
Authentication data (MAC value variable length field uses secret key shared by both parties)			

- Can use HMAC-MD5, HMAC-SHA
- SPI identifies a security association.
- Sequence number is 32 bit counter and if it exceeds 2^{32}, new SA will be needed.

ESP

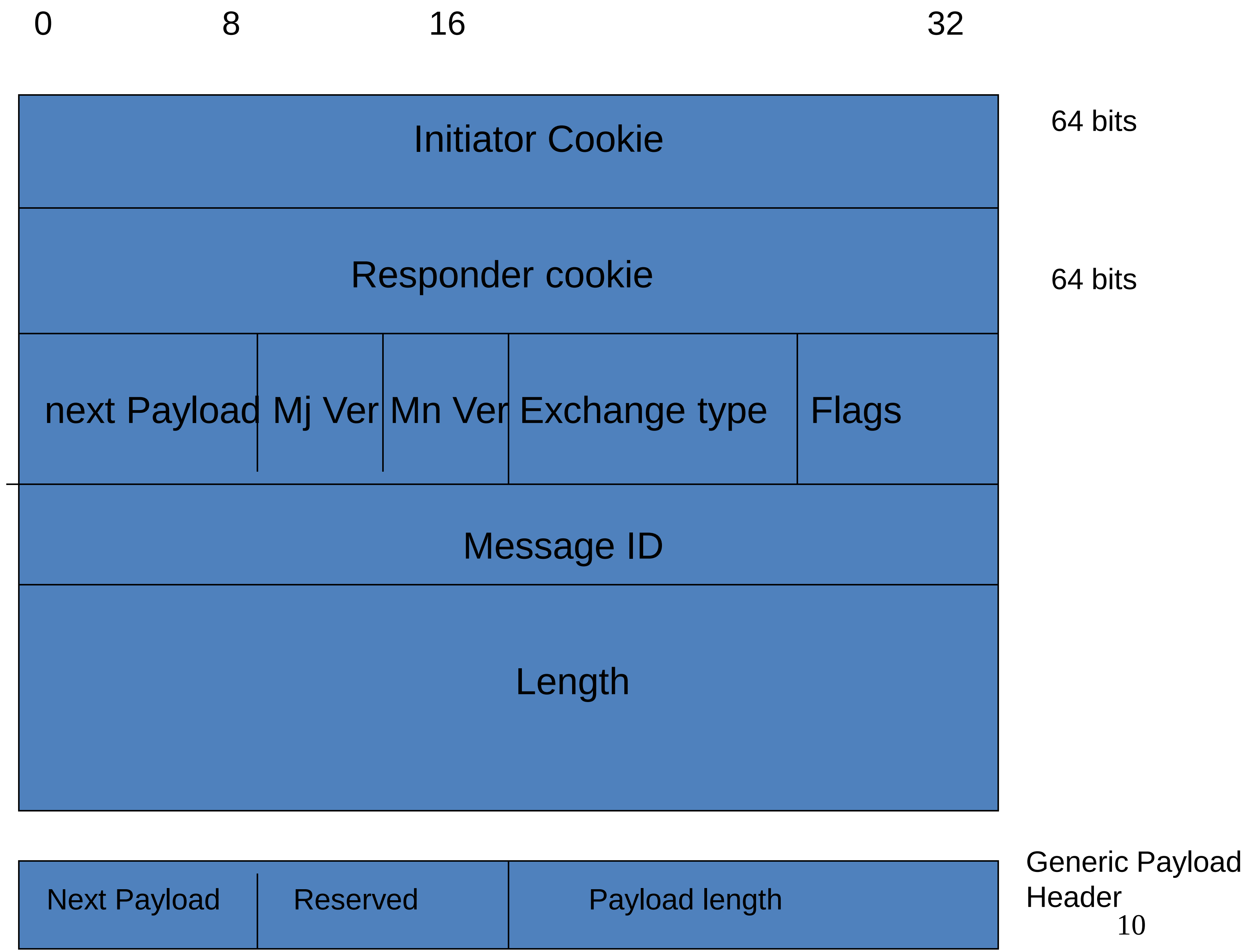


- Authentication covers cipher text plus ESP header
- Padding needed to cater for block ciphers

Key management

- ISAKMP (Internet Security association key management protocol)
- Oakley Key agreement protocol

ISAKMP Header



Algorithms used in IPSec

- HMAC-SHA1/SHA2 for integrity protection and authenticity.
- TripleDES-CBC for confidentiality
- AES-CBC for confidentiality.
- AES-GCM providing confidentiality and authentication together efficiently.

Attacks on IPSec

- S. Vaudenay, Security flaws induced by CBC padding – padding oracle attack on CBC mode
- Server gives ‘’invalid padding’’ instead of ‘’encryption failure’’.
- Bleichenbacher oracles on IKEv1 implementation on PKCSv1
- Attacker issues queries to server a number of times to guess key bytes.
- For a AES key, 4096 queries need to be made in the worst case.
- SLOTH attacks (security losses from obsolete and truncated transcript hashes)
- FREAK atack (factoring RSA export keys)

Post Quantum cryptography

- Problems such as factorization, Discrete logarithm, EC (elliptic curve) Discrete logarithm can be solved by Shor’s algorithm
- Grover’s algorithm can be tackled using bigger key lengths.
- Hence NIST called for proposals for Encryption, Key exchange and digital signatures, authentication

Requirements for PQ IPSec

- The size of encryption keys and signatures.
- The time required to encrypt and decrypt on each end of a communication channel, or to sign messages and verify signatures.
- The amount of traffic sent over the wire required to complete encryption or decryption or transmit a signature for each proposed alternative.

PQ cryptoalgorithms

- Five approaches
- (a) Learning with Errors (lattice based) (in a n-dimensional vector space closest vector problem, shortest vector problem, NTRU)
- (b) Isogeny on Elliptic curves for key exchange
- (c)Code based cryptography McEliece and Neiderwriter use Error correction codes to derive public and private keys with purposefully injected errors)
- (d) Multivariate quadratic equations
- (e) Hash based signatures (Merkle trees)

Learning with errors problem

$$f_{\mathbf{x}}(\mathbf{a}) = a_0x_0 + \cdots + a_nx_n + \epsilon \mod q$$

$$\mathbf{pk} = \begin{bmatrix} a_{00} & a_{01} & \cdots & a_{0n} & y_0 \\ a_{10} & a_{11} & \cdots & a_{1n} & y_1 \\ & & \vdots & & \\ a_{n0} & a_{n1} & \cdots & a_{nn} & y_n \end{bmatrix}$$

$$\mathbf{sk} = (s_0, s_1, \ldots, s_n)$$

To encrypt a bit , choose randomly the columns and embed m in the last coordinate of the result by adding 0 or q/2.

Comparison of various methods for Signatures and Key exchange

	Signatures	Key Exchange	Fast?
Elliptic Curves	64 bytes	32 bytes	✓
Lattices	2.7kb	1 kb	✓
Isogenies	✗	330 bytes	✗
Codes	✗	1 mb	✓
Hash functions	41 kb	✗	✓

MICROSOFT

- Two signature schemes and two key exchange schemes
- **FrodoKEM**

FrodoKEM is based upon the Learning with Errors problem, which is, in turn, based upon lattices.

- **SIKE**

SIKE (Supersingular Isogeny Key Encapsulation) uses arithmetic operations of elliptic curves over finite fields to build a key exchange.

- **Picnic**

Picnic is a public-key digital signature algorithm, based on a zero-knowledge proof system and symmetric key primitives.

- **qTESLA**

qTESLA is a post-quantum signature scheme based upon the Ring Learning With Errors (R-LWE) problem.

CONCLUSION

- Implementations on VLSI, FPGA, GPUs are being optimized
- Cryptanalysis by peers is being done.
- NIST hopes that more than one suite can be selected for different applications
- IPSec is expected to use these in the next decade