Python and Crypto: Hash to Obtain Random Subset (HORS)

Prof Bill Buchanan OBE, The Cyber Academy

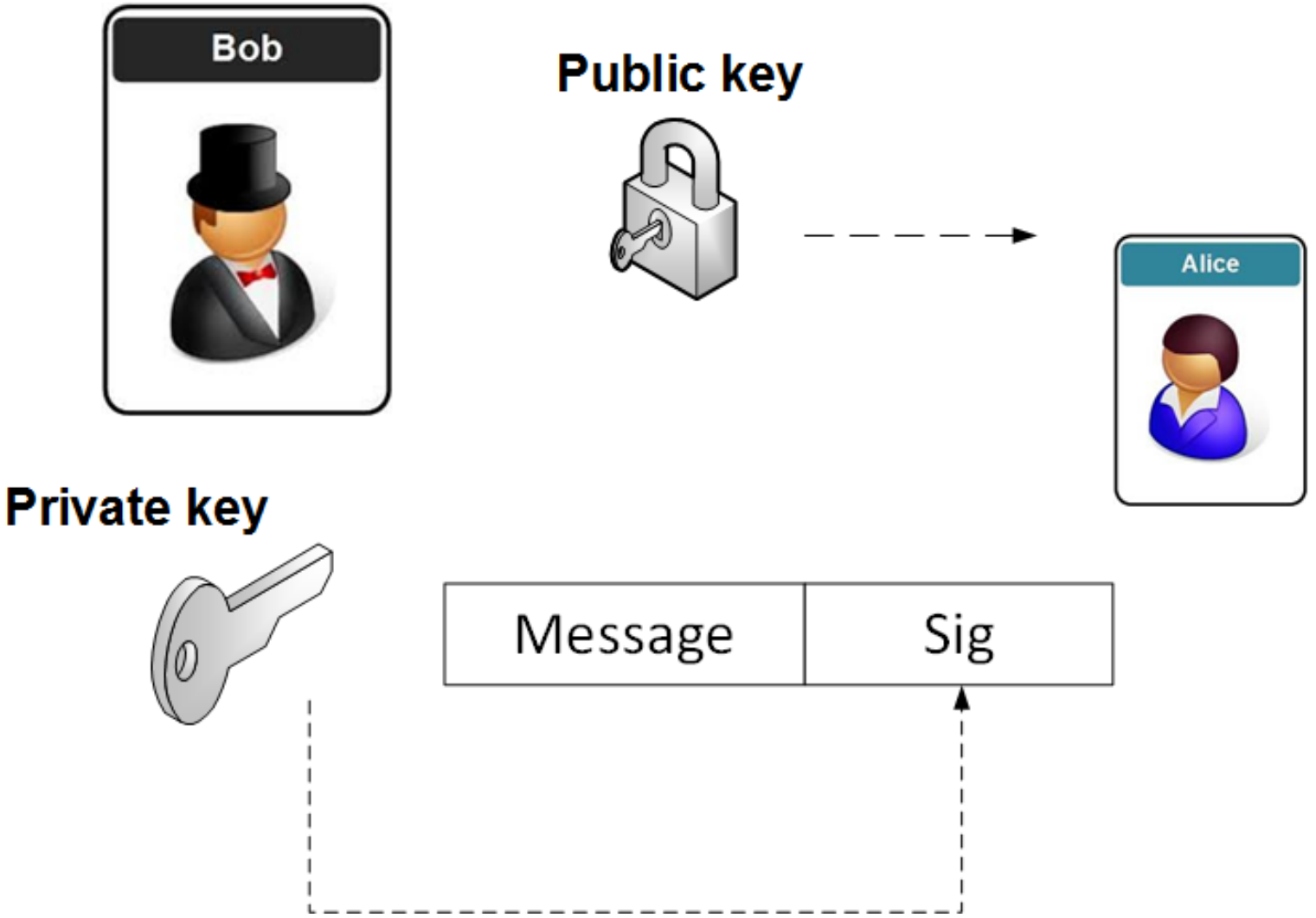
http://asecuritysite.com

CYBER ACADEMY

Quantum Methods

- Quantum Computers will crack most public key methods, such as RSA and Elliptic Curve encryption.
- We need new methods which define hard problems which will not be cracked by quantum computers.
- **Lattice-based cryptography** [Lattice] – This classification shows great potential and is leading to new cryptography, such as for fully homomorphic encryption [here], and code obfuscation. An example is given in the following section.
- **Code-based cryptography** [McEliece] – This method was created in 1978 with the McEliece cryptosystem but has barely been using in real applications. The McEliece method uses linear codes that are used in error correcting codes, and involves matrix-vector multiplication. An example of a linear code is Hamming code [here].
- **Multivariate polynomial cryptography** [UOV] – These focus on the difficulty of solving systems of multivariate polynomials over finite fields. Unfortunately, many of the methods that have been proposed have already been broken.
- **Hash-based signatures** [GMSS] – This would involve created digital signatures using hashing methods.

Hash-based signatures



Hash-based Signatures

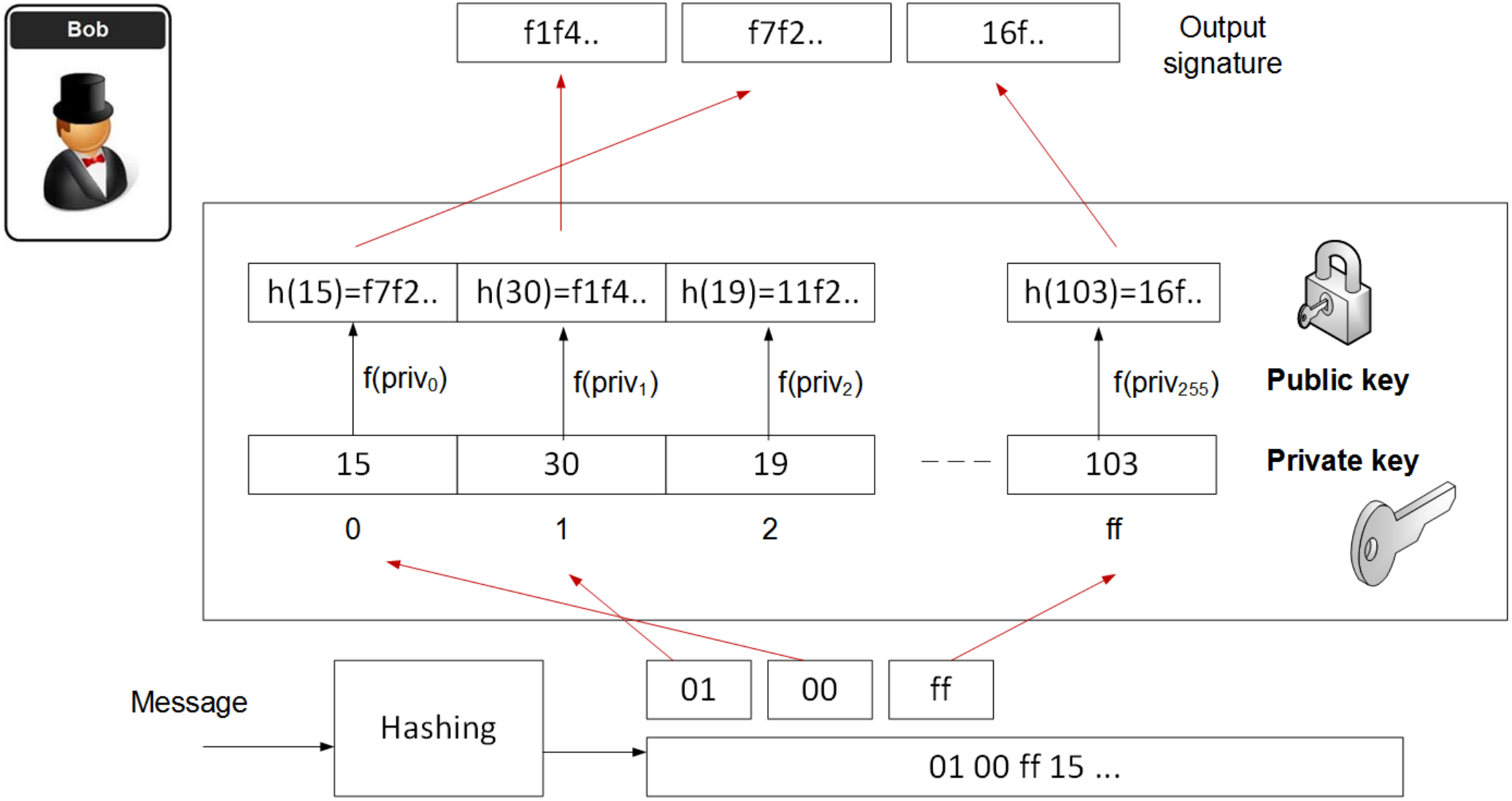
One-time signatures:

- **Lamport One-Time Signature**. Lamport. Outlines Lamport signatures.
- **Winternitz One-Time Signature (WOTS/WOTS+)**. Winternitz. Outlines Winternitz signatures.
- **Hash to Obtain Random Subset (HORS) Signatures**. HORS Signature. HORS signatures.

Trees:

- **Extended Merkle Signatures Scheme (XMSS)**. Merkle Signature. Outlines Merkle signatures.
- **SPHINCS**. SPHINCS. Outlines SPHINCS.
- **HORST** (HORS with Trees).

Hash to Obtain Random Subset (HORS)



Python and Crypto: Hash to Obtain Random Subset (HORS)

Prof Bill Buchanan OBE, The Cyber Academy

http://asecuritysite.com

CYBER ACADEMY