# Introduction to Cryptology

# 12.2 - A Hash-based Signature, and Pairings

Federico Pintore
Mathematical Institute, University of Oxford (UK)

UNIVERSITY OF OXFORD

Michaelmas term 2020

# Hash-based Signatures

No reliance on number-theoretic hardness assumptions.

Security proofs given in the standard model.

Believed to be post-quantum secure.

# Lamport's Signature Scheme

Proposed by Leslie Lamport in 1979.

It is a one-time secure signature scheme.

One-time security: $\mathcal{A}$ can query the signing oracle on one message in the $\mathrm{Sig}^{\mathrm{forge}}_{\mathcal{A},S}(n)$ experiment.

One-time secure signature schemes are usually used as building blocks for other cryptosystems.

# Lamport's Signature Scheme

Example (Katz-Lindell book)

- Consider a **3-bit** message $m = \mathbf{011}$ and a hash function $H$.
- Let the private key and public key be as follows:

$$\mathrm{SK} = \begin{pmatrix} x_{1,0} & x_{2,0} & x_{3,0} \\ x_{1,1} & x_{2,1} & x_{3,1} \end{pmatrix} \quad \mathrm{PK} = \begin{pmatrix} y_{1,0} & y_{2,0} & y_{3,0} \\ y_{1,1} & y_{2,1} & y_{3,1} \end{pmatrix},$$

  where $\{x_{i,j}\}$ are chosen uniformly at random from $\{0,1\}^n$ and $y_{i,j} = H(x_{i,j})$, for $i = 1,2,3$ and $j = 0,1$.
- The signature is $\sigma = (x_{1,\mathbf{0}}, x_{2,\mathbf{1}}, x_{3,\mathbf{1}})$.
- The verification-algorithms checks if

$$H(x_{1,\mathbf{0}}) \stackrel{?}{=} y_{1,0} \quad H(x_{2,\mathbf{1}}) \stackrel{?}{=} y_{2,1} \quad H(x_{3,\mathbf{1}}) \stackrel{?}{=} y_{3,1}$$

# Lamport's Signature Scheme

Given a hash function $H$, the Lamport's signature scheme (KeyGen, Sign, Verify) for messages of length $\ell(n)$ is defined as follows.

- $(\mathrm{PK}, \mathrm{SK}) \leftarrow \mathrm{KeyGen}(n)$: on input a security parameter $n$, it sets

  $$\mathrm{PK} = \begin{pmatrix} x_{1,0} & x_{2,0} & \dots & x_{\ell,0} \\ x_{1,1} & x_{2,1} & \dots & x_{\ell,1} \end{pmatrix} \quad \mathrm{SK} = \begin{pmatrix} y_{1,0} & y_{2,0} & \dots & y_{\ell,0} \\ y_{1,1} & y_{2,1} & \dots & y_{\ell,1} \end{pmatrix},$$

  where $\{x_{i,j}\}$ are chosen uniformly at random from $\{0,1\}^n$ and $y_{i,j} = H(x_{i,j})$, for $i = 1, \dots, \ell$ and $j = 0, 1$.
- $\mathrm{Sign} \leftarrow \mathrm{Sign}(\mathrm{SK}, m \in \{0,1\}^\ell)$: the signature $\sigma$ is set to $(x_{1,m_1}, \dots, x_{\ell,m_\ell})$, where $m = m_1 \dots m_\ell$.
- $\mathrm{Verify}(\mathrm{PK}, m, \sigma)$: given a public key, a message $m_1 \dots m_\ell$ and a signature $\sigma = (\sigma_1, \dots, \sigma_\ell)$, it outputs 1 if $H(\sigma_i) = y_{i,m_i} \quad \forall i \in \{1, \dots, \ell\}$, 0 otherwise.

# Lamport's Signature Scheme

In the security game, $\mathcal{A}$ can learn only one signature on a message $m$ of their choice.

$\mathcal{A}$ has to output a signature on a new message $m'$. The signature will then involve some new $x_{i,j}$, say $x_{1,1}$.

If the forged signature is valid, $\mathcal{A}$ managed to compute the preimage of $y_{1,1}$, that is part of the public key.

This cannot happen if $H$ is a preimage-resistant hash function.

# Security of Lamport's Signature Scheme

Theorem

*If $H$ is a preimage-resistant hash function, then the Lamport's signature scheme is one-time secure.*

# Bilinear Maps (Pairings)

Let $\mathbb{G}_1, \mathbb{G}_2$ and $\mathbb{G}_T$ be three groups of the same prime order $p$.

A pairing is an efficiently computable function

$$e : \mathbb{G}_1 \times \mathbb{G}_2 \rightarrow \mathbb{G}_T$$

satisfying the following conditions:

- $e(g_1^a, g_2^b) = e(g_1, g_2)^{ab}$, for every $g_1 \in \mathbb{G}_1, g_2 \in \mathbb{G}_2$ and $a, b \in \mathbb{Z}_p$;
- if $g_1$ is a generator of $\mathbb{G}_1$ and $g_2$ is a generator of $\mathbb{G}_2$, then $e(g_1, g_2)$ is a generator of $\mathbb{G}_T$ (non-degeneracy).

# Pairing-based Signatures

The Tate/Weil pairing maps pairs of elements of elliptic-curve groups to elements of the multiplicative group of a finite field.

# Pairing-based Signatures

The Tate/Weil pairing maps pairs of elements of elliptic-curve groups to elements of the multiplicative group of a finite field.

- Boneh-Lynn-Shacham signature scheme (2004).
  - PK $= (\mathbb{G}_1 = \mathbb{G}_2, \mathbb{G}_T, p, g, h := g^x, H)$, SK $:= (x, H)$, where $H : \{0,1\}^* \to \mathbb{G}_1$;
  - the signature $\sigma$ on a message $m$ is $H(m)^x$;
  - the verification algorithm checks whether $e(\sigma, g) = e(H(m), h)$.
- Boneh-Boyen signature scheme (2004)

# Further Reading I


Carlisle Adams and Steve Lloyd.
Understanding PKI: concepts, standards, and deployment considerations.
Addison-Wesley Professional, 2003.

Dan Boneh, Ben Lynn, and Hovav Shacham.
Short signatures from the Weil pairing.
Journal of cryptology, 17(4):297–319, 2004.

Tim Dierks.
The transport layer security (TLS) protocol version 1.2.
2008.

Carl Ellison and Bruce Schneier.
Ten risks of PKI: What you're not being told about public key infrastructure.
Comput Secur J, 16(1):1–7, 2000.

# Further Reading II


Amos Fiat and Adi Shamir.
How to prove yourself: Practical solutions to identification and signature problems.
In Advances in Cryptology—CRYPTO'86, pages 186–194. Springer, 1987.

Martin Georgiev, Subodh Iyengar, Suman Jana, Rishita Anubhai, Dan Boneh, and Vitaly Shmatikov.
The most dangerous code in the world: validating SSL certificates in non-browser software.
In Proceedings of the 2012 ACM conference on Computer and communications security, pages 38–49. ACM, 2012.

# Further Reading III


Hugo Krawczyk.
Cryptographic extraction and key derivation: The HKDF scheme.
In Annual Cryptology Conference, pages 631–648. Springer, 2010.

Hugo Krawczyk, Kenneth G Paterson, and Hoeteck Wee.
On the security of the TLS protocol: A systematic analysis.
In Advances in Cryptology–CRYPTO 2013, pages 429–448. Springer, 2013.

Leslie Lamport.
Constructing digital signatures from a one-way function.
Technical report, Technical Report CSL-98, SRI International Palo Alto, 1979.