RSA-PSS

Provable Secure RSA Signatures
and their Implementation

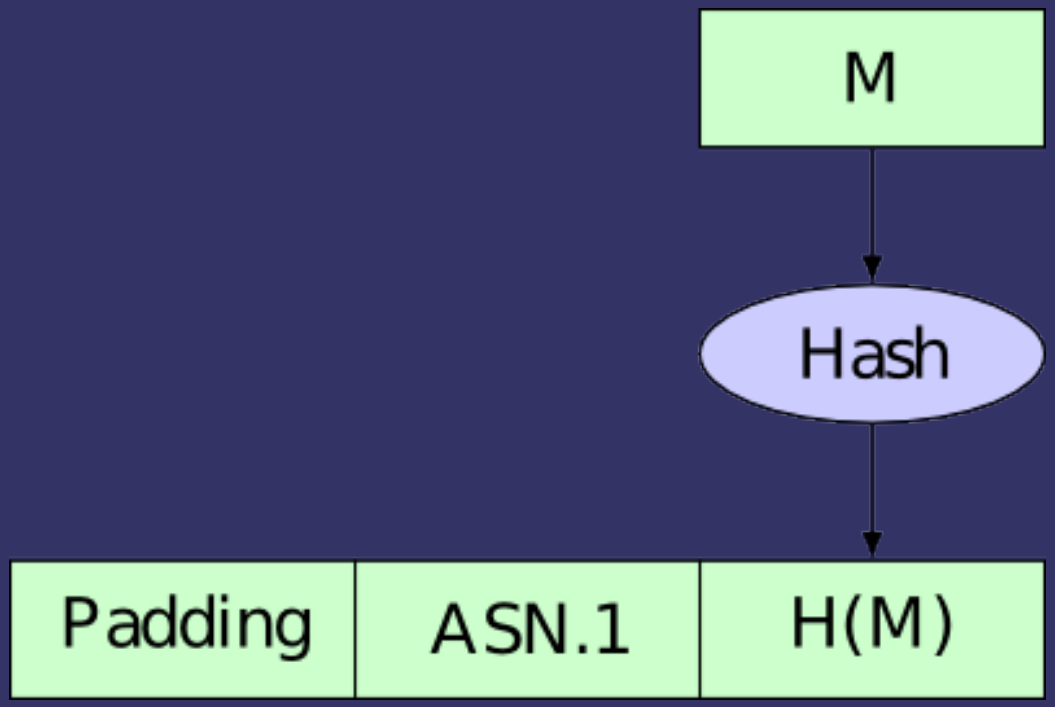
Overview

- What is RSA-PSS?
- Why RSA-PSS?
- Comparing original and standardized PSS
- Status of Protocols, Standards and Implementations
- RSA-PSS in X.509
- Algorithmenkatalog

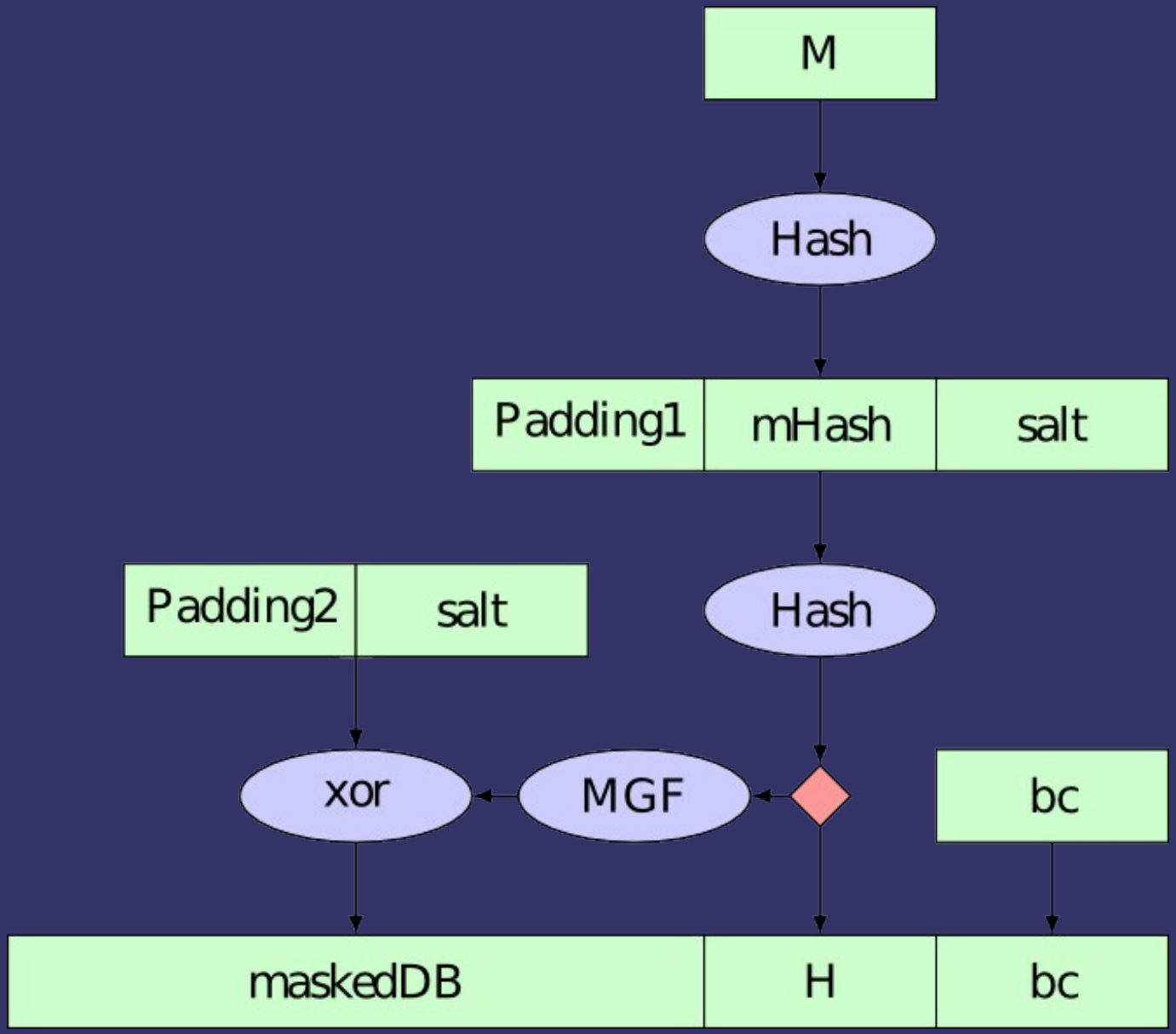
RSA

- Public key cryptosystem
- Invented 1977 by Ron Rivest, Adi Shamir, Leonard Adleman
- Public Key *(e, N)*, private key *(d, N)* with $(X^{de}) \bmod N = X$
- Encrypt: $E = (M^e) \bmod N$,
  Decrypt: $M = (E^d) \bmod N$
- Sign: $S = (M^d) \bmod N$,
  Verify: $M = (S^e) \bmod N$
- What is M?

Hash-then-sign, PKCS #1 v1.5



Probabilistic Signature Scheme



Probabilistic Signature Scheme

- Developed 1996 by Mihir Bellare and Phil-ipp Rogaway
- “Provable Secure” in the random oracle model
- That means: Secure if hash function is ideal, factoring is hard and RSA itself is as hard as factoring
- Uses a salt (randomization) and uses full size of RSA input

Status of PSS in standards

- RSASSA-PSS primitives are part of IEEE P1363a and PKCS #1 v2.1 / RFC 3447
- RSASSA-PSS supported by standards for X.509 (RFC 4055), CMS (RFC 4055)
- Not supported in OpenPGP, DNSSEC, XM-LDsig, TLS

X.509 Implementations

- Latest OpenSSL 1.0.0d: bare PSS signatures supported, no support for X.509
- X.509 Support in OpenSSL 1.1 CVS (not yet released
- Latest Mozilla nss / Firefox: Not supported
- I created patches for nss in the Google Summer of Code 2010, not yet merged
- Microsoft Windows (since Vista) supports X.509 with RSASSA-PSS
- Microsoft was faster than any other browser vendor in implementing an open standard!!

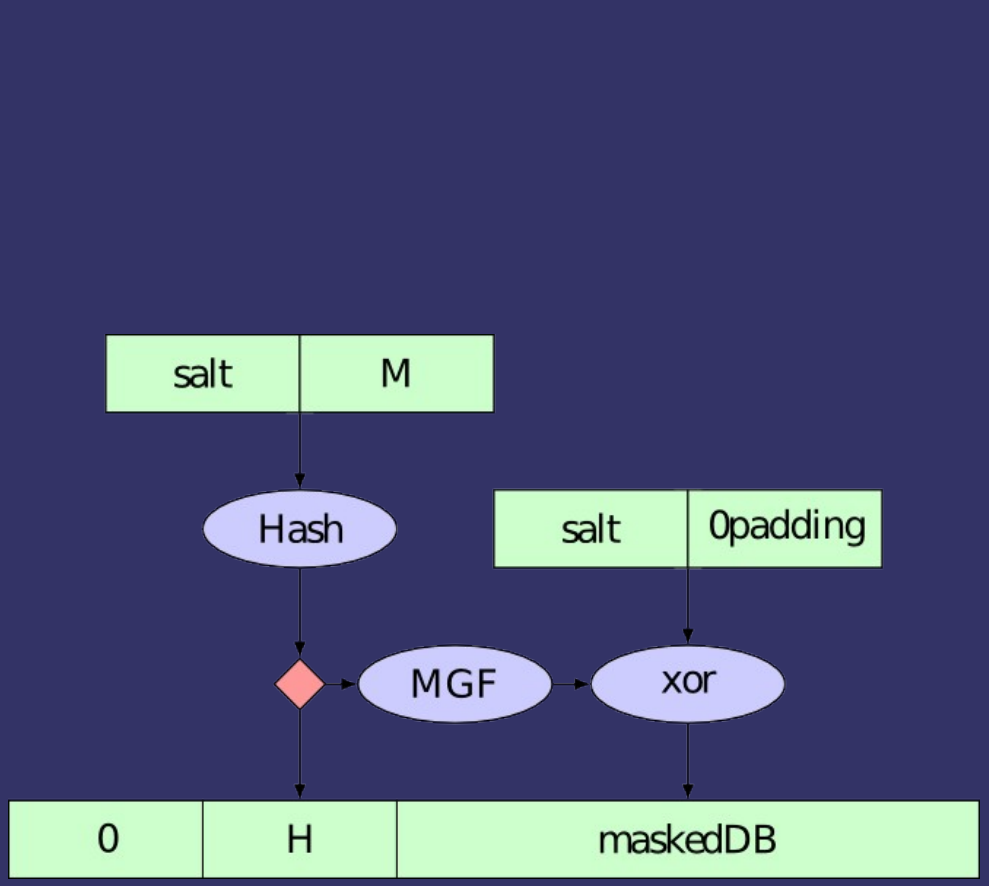
X.509 online test

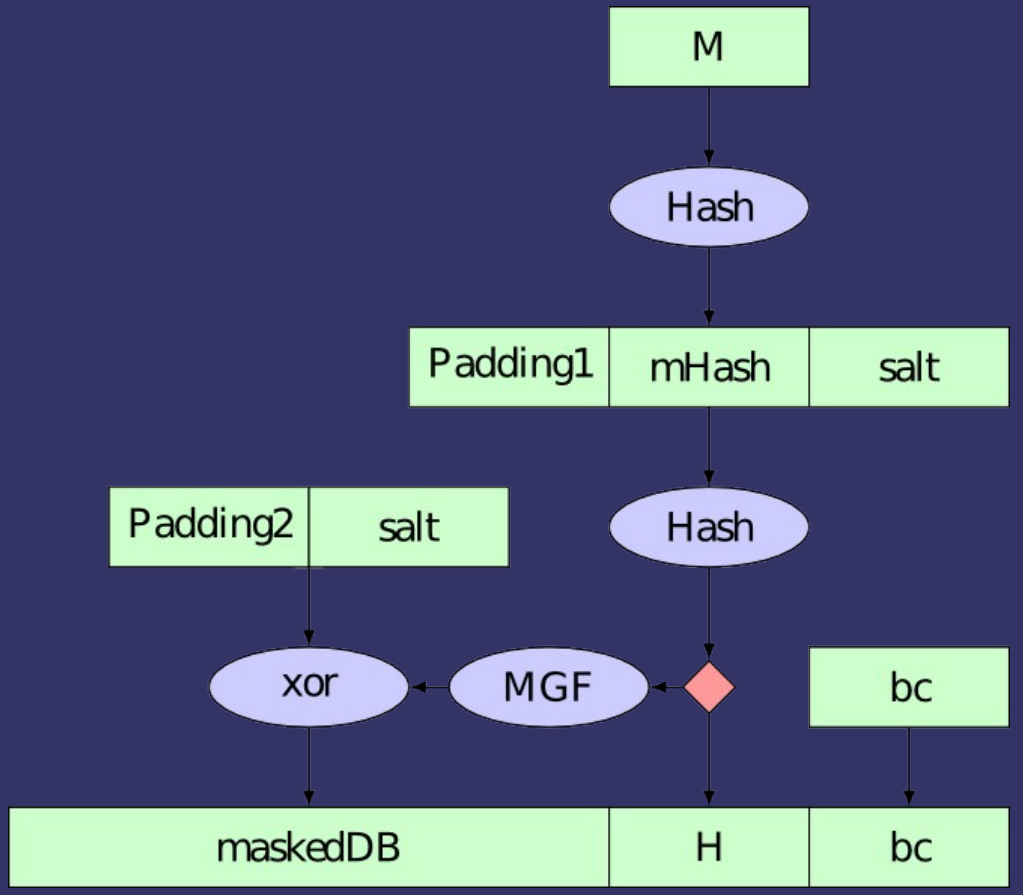
- http://ssl.hboeck.de/

Hashing

- A lot has happened in hash function research in recent years
- MD5 collision in 2004
- SHA-1: Collision attacks with a complexity of 2^{63}
- Successful fake of a CA certificate in 2008 (25C3, calculated on a PS3 cluster)
- SHA-3 competition running

PSS96 and PKCS #1 v2.1





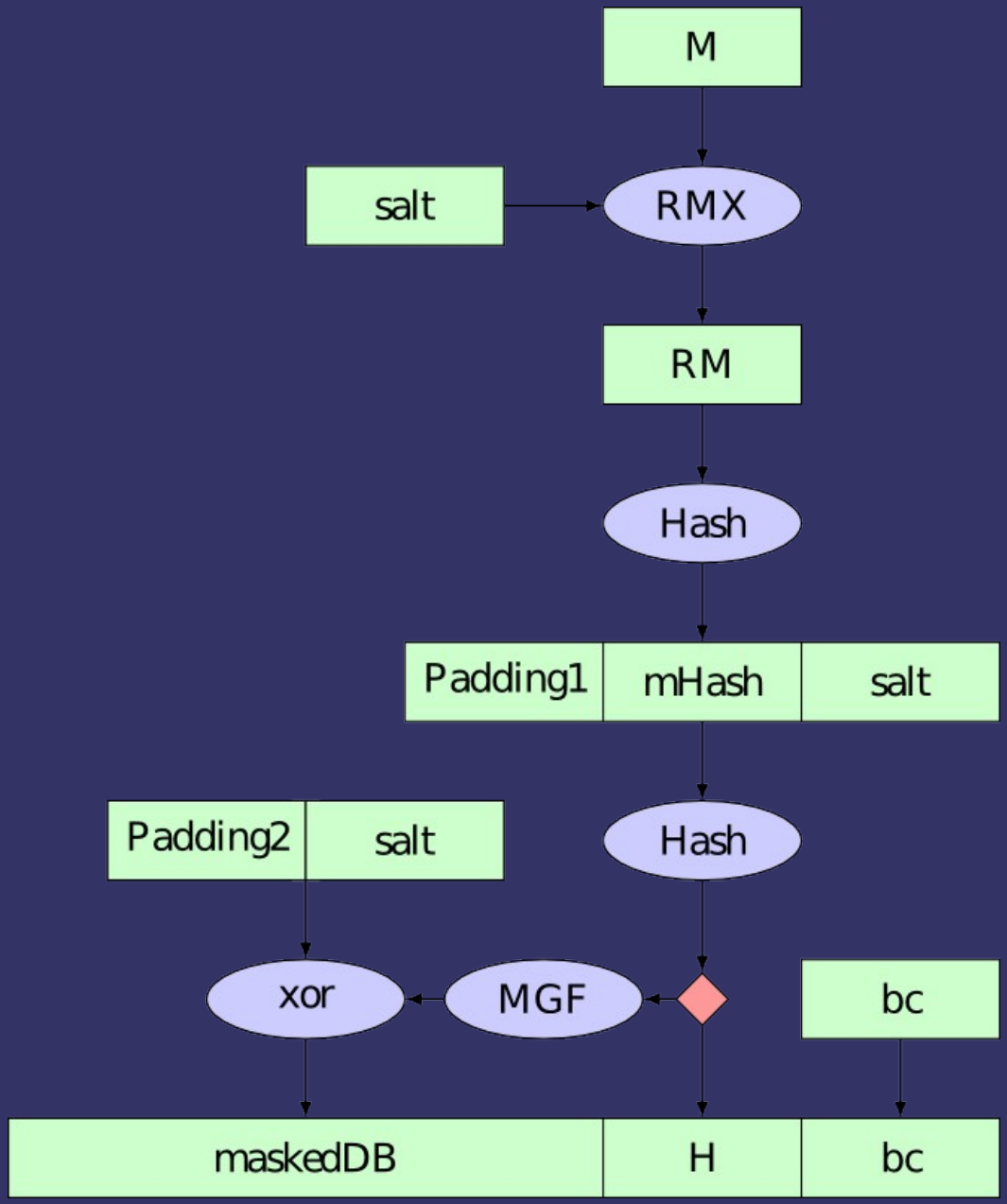
Input randomization

- Direct input randomization secures against possible collision flaws in the hash
- eTCR (enhanced Target Collision resistance)
- PSS96 provides eTCR, PSS from standars PKCS #1 v2.1 / IEEE 1363a does not
- Randomized hashing: brings back eTCR

Randomized Hashing

- Generate random value *rv*
- Repeat *rv* and XOR it with input message (XOR vigenere)
- Use *rv* || *(M* ⊕ *rv)* || *rv_length* as hash function input
- Problem: *rv* has to be shipped separately
- Randomized hashing and PSS: salt can be used as *rv*

PSS with randomized hashing



Algorithmenkatalog

- *Das Formatierungsverfahren RSA: „Signature Schemes with Appendix“ PKCS#1-v1_5 aus [15] Abschn. 8.2 und 9.2 ist noch bis Ende 2014 geeignet. Zum Erzeugen von Zertifikatssignaturen ist das PKCS#1-v1_5-Format darüber hinaus bis Ende 2016 geeignet. Es wird aber empfohlen, dieses Verfahren nicht über Ende 2013 hinaus zu verwenden.*

Algorithmenkatalog

- Good: Pushing for better security
- Bad: Not pushing for better standards and implementations
- Technische Richtlinie 03125 (long time archiving) requires algorithms from “Al-gorithmenkatalog”
- TR 03125 is based on XMLDsig
- XMLDsig does not support PSS!

Optional slide: Really provable?

- Is it possible to provide **really** provable security for public key cryptography?
- Not today: We don't know enough about complexity theory.
- Our whole trust in cryptography relies on assumptions – we believe that if nobody was able to break something in a long time, it must be secure.
- Is factoring hard? Is RSA as hard as factoring? Anyone with a Quantum computer out there?

Optional Slide: Really provable?

- But if we could:
  - Prove P != NP
  - Create trapdoor function out of FNP problem
  - Create cryptosystem and prove that we only hit the hard problems in our FNP problem
  - Create a provable secure scheme that is not based on a hypothetical ideal hash function, but a real one
  - Prove that the whole thing is also resistant to Quantum computers
- P != NP is considered to be one of the hardest problems in mathematics and the-oretical computer science – and that's only the first step.

RSA-PSS

- Questions? Discussion?

  Diploma thesis on RSA-PSS will be available at
  http://rsapss.hboeck.de/