Confined guessing:

a reduction strategy to obtain new signatures from standard assumptions

Florian Böhl[1], Dennis Hofheinz[2], Tibor Jager[3],
Jessica Koch[2], and Christoph Striecks[2]

[1] NXP, Leuven, Belgium
[2] Karlsruhe Institute of Technology, Germany
[3] Ruhr-Universität Bochum, Germany

Overview

- New techniques for designing signature schemes
- Result: new signature schemes from the CDH, RSA, and SIS assumptions in the standard model
- Core idea: revisit tag-based signatures

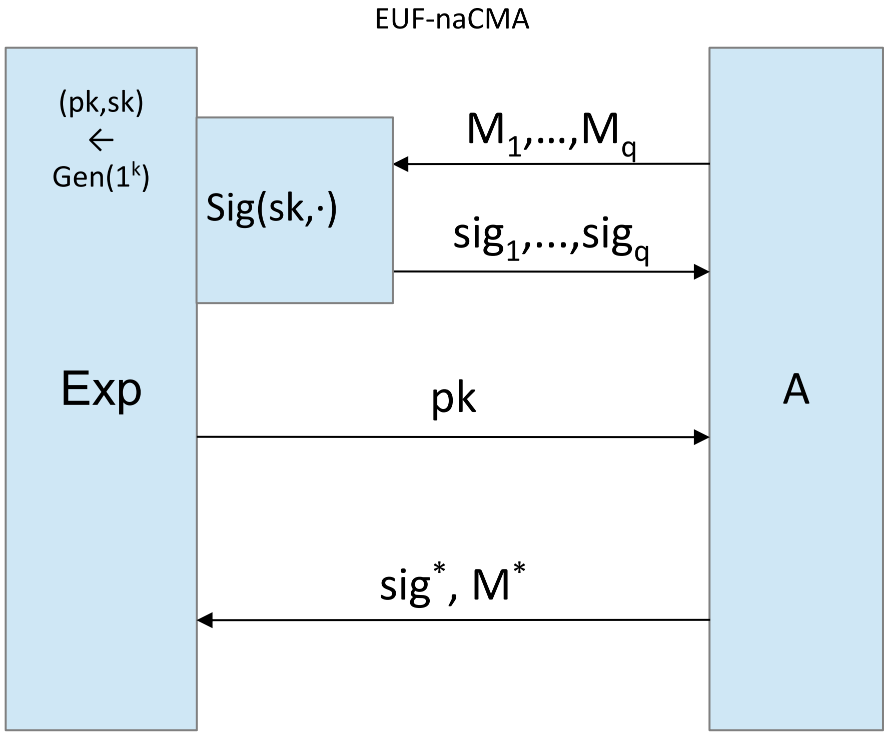
Digital signatures

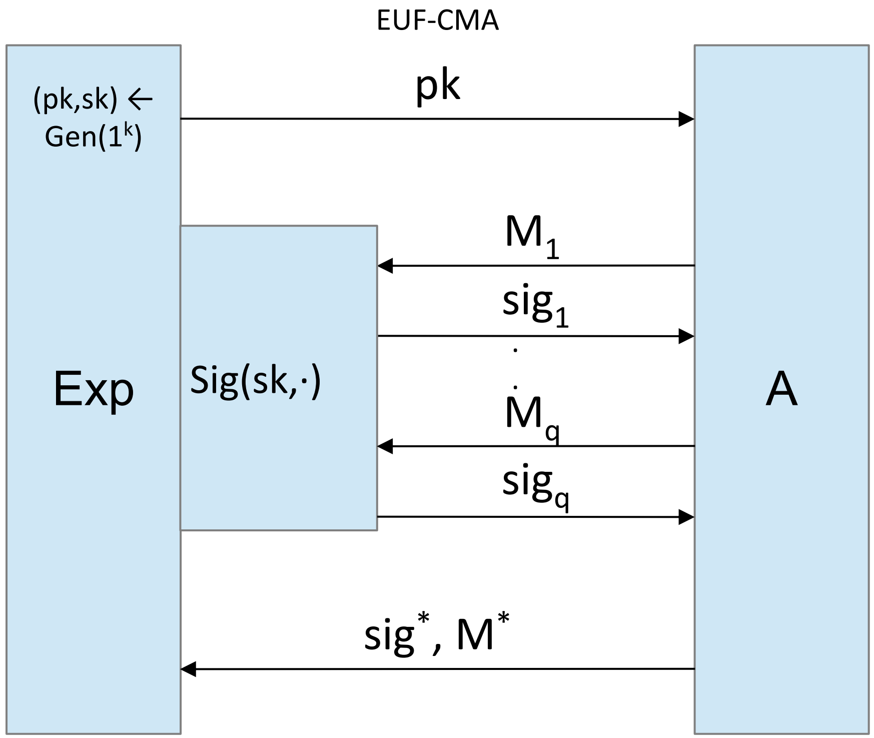
<u>SIG:</u>

- Gen(k): pk, sk
- Sig(sk,M): sig
- Ver(pk,M,sig): b (i.e., 1 or 0, valid or invalid)

- Application: HTTPS, OS system updates
- Generic: from OWF [L79,NY89,R90]
- Tree-based: RSA assump. [GMR88,CD95,CD96], later [CS99,F03, J08,HK08,HW09]
- Partitioning: e.g., [C00,W05,HK08,B10]
- Specific: SDH assump. [BB08], Dual Systems [W09], RO [BR93]

EUF-(na)CMA security





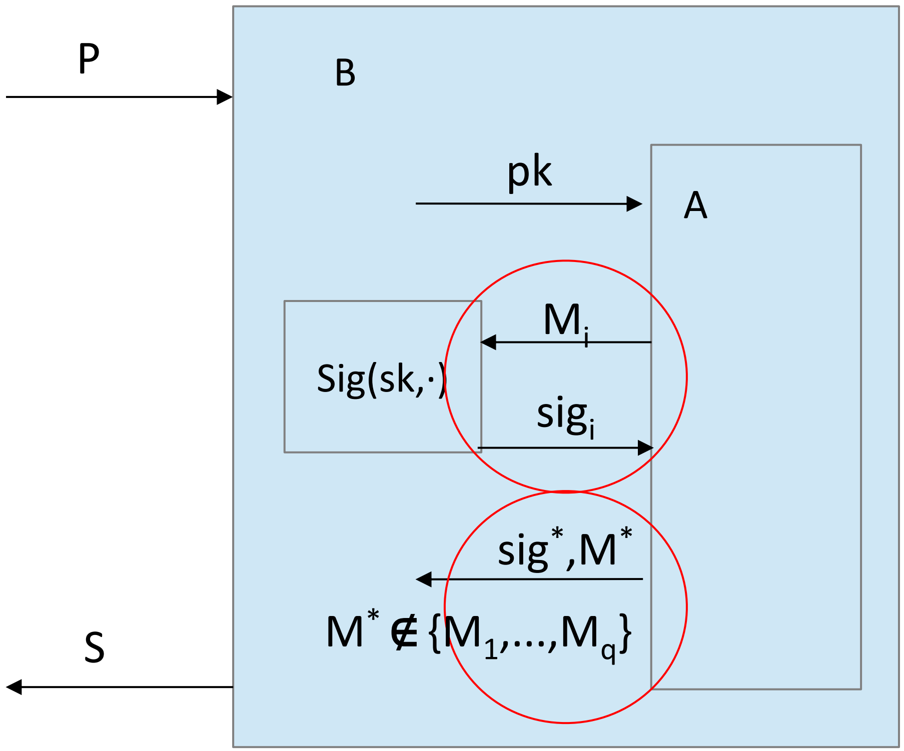
A wins iff $\mathrm{Ver}(pk,M^*,sig^*) = 1$ and $M^* \notin \{M_1,\ldots,M_q\}$,

SIG EUF-(na)CMA secure iff
Pr[A wins] negl.

Generic efficient transformation: EUF-naCMA to EUF-CMA [KR00] using chameleon hashes

The technical difficulty, or “the dilemma”

- Reduction: if A is successful then an alg. B solves (using A) an assumed-to-be-hard problem P
- Via: extract solution S from A-output (M*, sig*)



- Dilemma: B has to produce signatures for some *but* not all messages, i.e., *should not* be able to generate a signature for M*! (M* is not known to B in advance.)

- Hence: we need reduction strategies

Reduction strategies

- Specific reduction strategies are known, e.g., partitioning [BR96,C00,W05,HJK11] or dual systems [W09]
- But: many EUF-CMA-secure signature schemes under mild assumptions have large parameters:
  - e.g., [W05] under CDH: $|vk| \in O(k)$
- Our initial motivation:

  Can we construct an EUF-CMA-secure signature scheme under a standard assumption (e.g., CDH, RSA) with shorter parameters or more efficient computations?

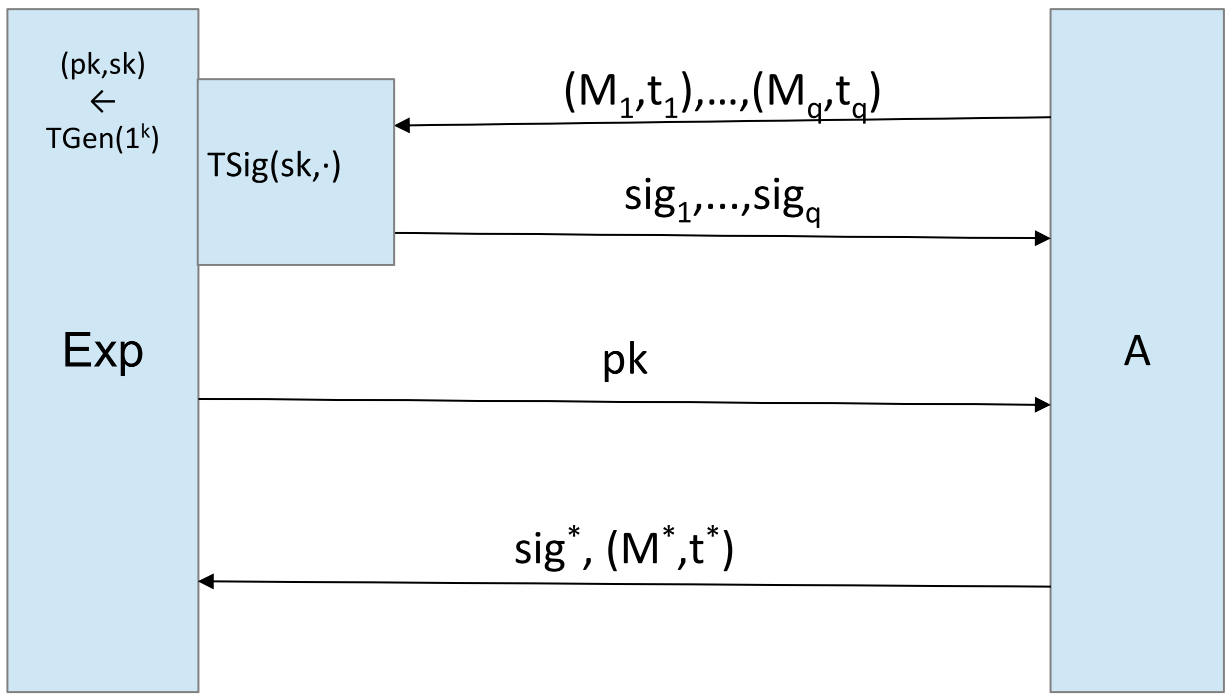
Revisit tag-based signatures

TSIG:

- Gen(k): pk, sk
- Sig(sk,M,t): sig
- Ver(pk,M,sig,t): b (i.e., 1 or 0)

- We define mild security for tag-based signatures

Mild security



A wins iff $Ver(pk,M^*,sig^*,t^*) = 1$ and $M^* \notin \{M_1,\ldots,M_q\}$ and $t^* \in \{t_1,\ldots,t_q\}$

and minor restrictions (distinct M_i, only m tag collisions),

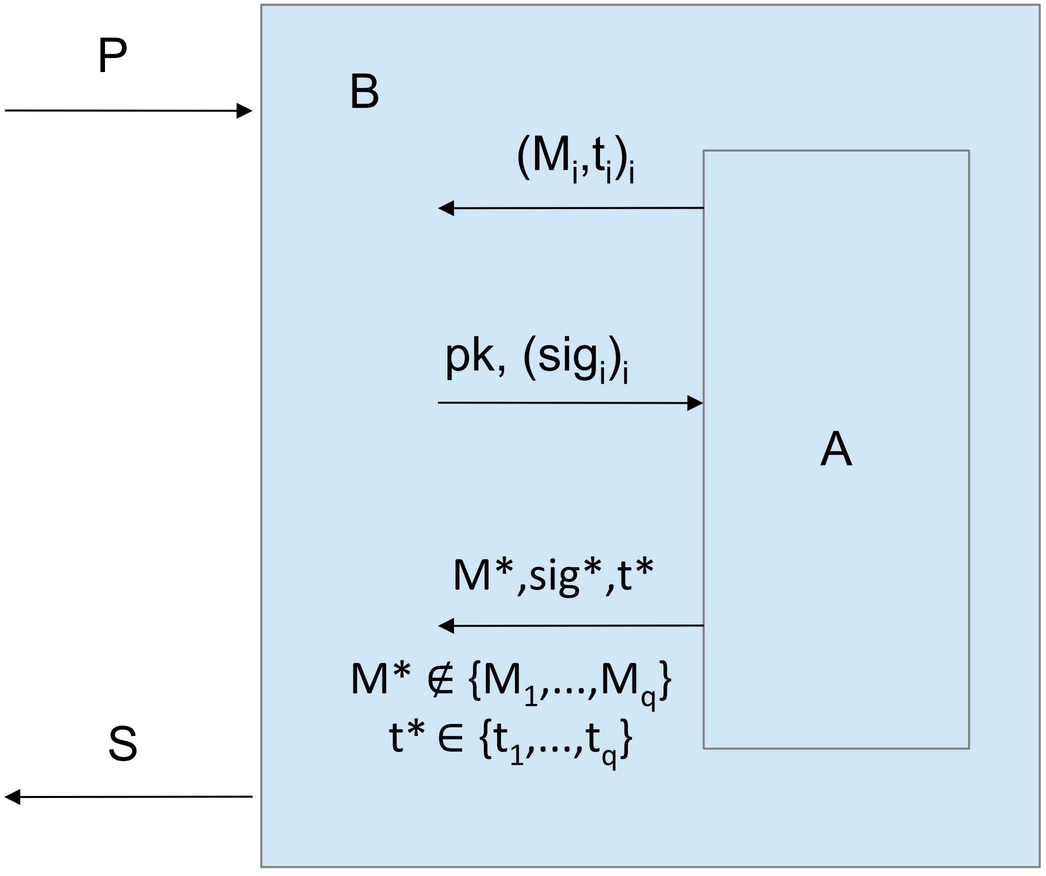
Observation: t^* from a set of polynomial size

Further: mildly secure tag-based signatures easier to achieve

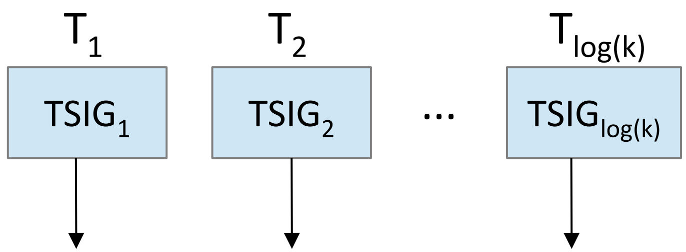
Starting with mild security

- A outputs msg-tag pairs
- A has to re-use a tag t*
- B can embed challenge into signature with tag t*
- Allow up to m tag-collisions for t*

- Mildly sec. schemes from CDH, RSA, SIS
- Adjust known schemes [BB04,HW09,B11]

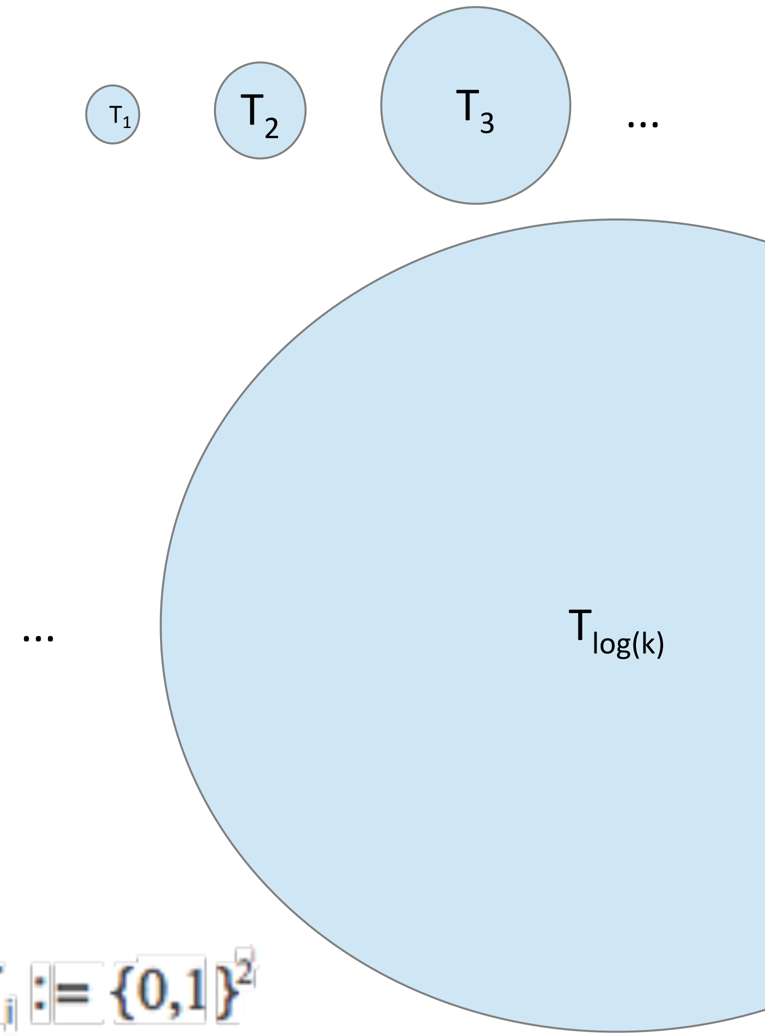


Confined guessing: from mild to full security



$$sig := (sig_{TSIG_1}, sig_{TSIG_2}, \ldots, sig_{TSIG_{\log(k)}})$$

$$(pk, sk) := (pk_{TSIG}, sk_{TSIG})$$



- log(k) mildly secure tag-based instances
- "connect" tags and messages (via a PRF)
- Crucial observation: there exist a tag set which is polynomial in k and has “not so many” tag collisions when picking tags unif. at random
- Procedure: find this tag set in reduction
- Similar techn. in different context: [BH12]

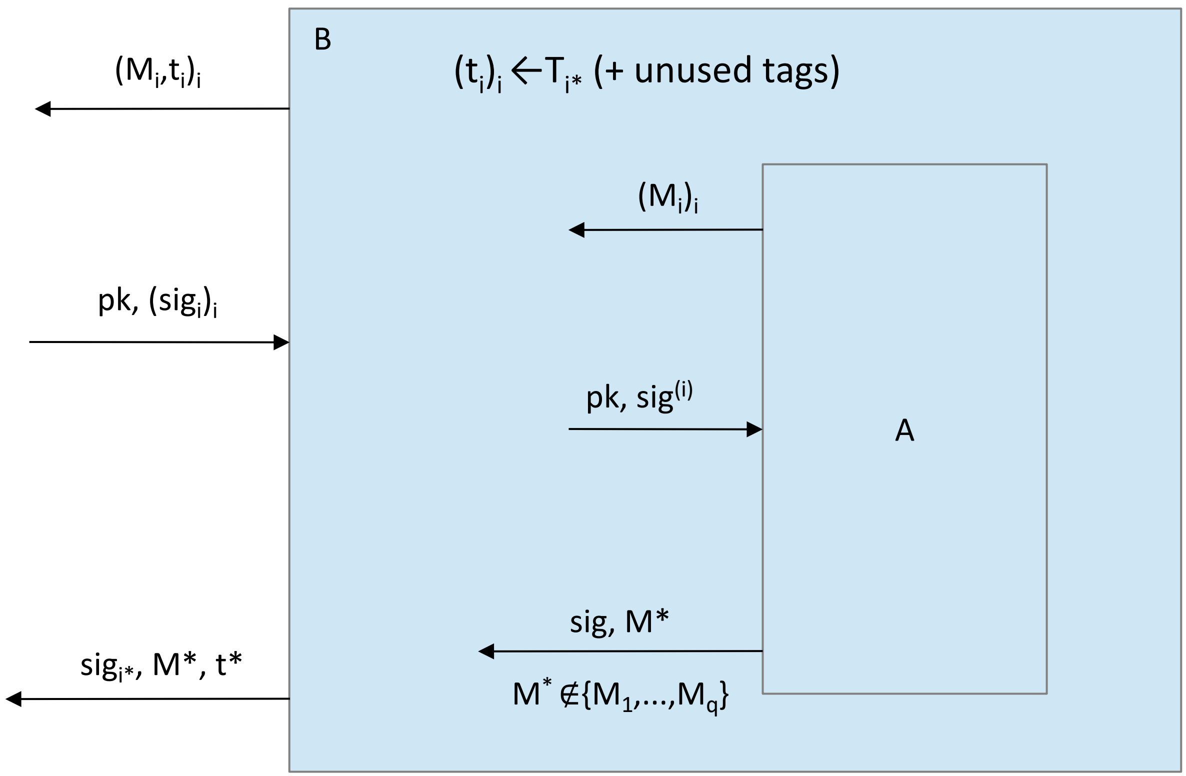
$$T_i := \{0,1\}^{2^i}$$

From mild to full security

- Key point: single out an instance i* such that
  (a) $|T_{i^*}|$ is poly and
  (b) Pr[m-tag-coll.] $\leq$ succ(A)/2
- Mildly secure tag-based schemes from CDH, RSA, SIS

->

- fully secure signatures from CDH, RSA, and SIS



$$sig = (sig_1, \ldots, sig_{i^*}, \ldots, sig_{\log(k)})$$

Conclusion and efficiency

- Result: new reduction strategy for designing signature schemes from CDH, RSA, and SIS (with optimizations) in the standard model

- Scheme's efficiency (with worse sec. red.):

assumpt.	pk size	sig. size	comments
CDH	$O(\log k)$	$O(1)$	more compact pks as [W05]
RSA	$O(1)$	$O(1)$	fewer gen. of large primes as [HW09,HJK11]
SIS	$O(m \cdot n)$	$O(\log k \cdot m)$	altern. to [B11]