# Accepted Manuscript


Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares

Benoît Libert, Marc Joye, Moti Yung

PII: S0304-3975(16)00162-6
DOI: http://dx.doi.org/10.1016/j.tcs.2016.02.031
Reference: TCS 10671

To appear in: *Theoretical Computer Science*

Received date: 6 November 2015
Accepted date: 23 February 2016

Please cite this article in press as: B. Libert et al., Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares, *Theoret. Comput. Sci.* (2016), http://dx.doi.org/10.1016/j.tcs.2016.02.031

# Born and raised distributively: Fully distributed non-interactive adaptively-secure threshold signatures with short shares[☆]

Benoît Libert

*Ecole Normale Supérieure de Lyon, Lyon, France*

Marc Joye

*Technicolor and Ecole normale supérieure, Los Altos, CA, USA*

Moti Yung

*Snapchat and Columbia University, New York, NY, USA*

**Abstract**

Threshold cryptography is a fundamental distributed computational paradigm for enhancing the availability and the security of cryptographic public-key schemes. It does it by dividing private keys into $n$ shares handed out to distinct servers. In threshold signature schemes, a set of at least $t+1 \leq n$ servers is needed to produce a valid digital signature. Availability is assured by the fact that any subset of $t+1$ servers can produce a signature when authorized. At the same time, the scheme should remain robust (in the fault tolerance sense) and unforgeable (cryptographically) against up to $t$ corrupted servers; *i.e.*, it adds quorum control to traditional cryptographic services and introduces redundancy. Originally, most practical threshold signatures have a number of demerits: They have been analyzed in a static corruption model (where the set of corrupted servers is fixed at the very beginning of the attack); they require interaction; they assume a trusted dealer in the key generation phase (so that the system is not fully distributed); or they suffer from certain overheads in terms of storage (large share sizes).

In this paper, we construct practical *fully distributed* (the private key is born distributed), non-interactive schemes —where the servers can compute their partial signatures without communication with other servers— with adaptive security (*i.e.*, the adversary corrupts servers dynamically based on its full view of the history of the system). Our schemes are very efficient in terms of computation, communication, and scalable storage (with private key shares of size $O(1)$, where certain solutions incur $O(n)$ storage costs at each server). Unlike other adaptively secure schemes, our schemes are erasure-free (reliable erasure is hard to assure and hard to administer properly in actual systems). To the best of our knowledge, such a fully distributed highly constrained scheme has been an open problem in the area. In particular, and of special interest, is the fact that Pedersen's traditional distributed key generation (DKG) protocol can be safely employed in the initial key generation phase when the system is born —although it is well-known not to ensure uniformly distributed public keys. An advantage of this is that this protocol only takes one round optimistically (in the absence of faulty player).

*Keywords:* Threshold signatures, fully distributed schemes, non-interactivity, adaptive security, efficiency, availability, fault tolerance, distributed key generation, erasure-freeness.

[☆]This is the full version of a paper published at PODC 2014. It includes all proofs that were not included in the proceedings version.

*Email addresses:* benoit.libert@gmail.com (Benoît Libert), marc.joye@gmail.com (Marc Joye), moti@cs.columbia.edu (Moti Yung)