Experimental Results on Secret Key Extraction from a UWB Channel

Enrico Paolini and Marco Chiani
Department of Electrical, Electronic, and Information Engineering "G. Marconi"
University of Bologna, via Venezia 52, 47521 Cesena (FC), Italy
Email: e.paolini@unibo.it, marco.chiani@unibo.it

I. Extended Abstract

KEY generation and distribution has always represented a fundamental issue in cryptography applications. To avoid the high computational cost of Rivest Shamir Adleman (RSA) systems (e.g., in the case of wireless devices with limited computational capability), several studies have focused on the possibility to achieve confidentiality by exploiting the physical channel between two end-points, usually called *Alice* (A) and *Bob* (B), in order to generate and distribute the key. According to the reciprocity theorem, in fact, the communication channel is expected to represent a common source of information for A and B, potentially exploitable to extract the same key to be used to share secret information reliably. A fundamental condition to achieve confidentiality via physical layer is that, due for example to spatial diversity, an eavesdropper experiences a different channel and is then prevented from generating the same key. Following standard nomenclature, the eavesdropper is here called *Eve* (E).

The ultra-wideband (UWB) technology, owing to its very high time resolution (in the order of nanoseconds) and to its capability to resolve multipath can provide a fine and accurate measurement of the channel response and can be favorably employed for secret key extraction even in indoor environments. A possible scheme for secret key extraction from the UWB physical channel comprises the following steps:

- *Channel probing*: a time slot is set as half of the channel coherence time. In the first slot, A transmits a data sequence to B. In the second slot, B transmits the same sequence back to A;
- *Quantization*: A and B convert their received waveforms into raw keys using the same quantization scheme;
- *Synchronization*: A and B remove synchronization (i.e., alignment) errors from their raw keys;
- *Reconciliation*: A and B remove substitution errors (i.e., bit discrepancies) from their raw keys;
- *Privacy amplification*: a shorter key is generated with a higher level of randomness, using hash functions.

Experimental results reported in the literature have highlighted how the UWB technology may confidently be used in the framework of physical layer security for key generation and distribution, especially in indoor environments with dense multipath. The aim of the talk will be to provide further experimental evidence about the feasibility of a procedure (validated in a step-by-step fashion) to extract the secret key from the UWB channel physical parameters. Note that only measurements collected in a real indoor environment are exploited in our analysis. In the process, some important aspects not fully addressed in previous works are investigated, such as a comparison between different quantization schemes or raw key alignment after quantization. As pointed out at the end of the paper, given the obtained A-B and A-E mismatch percentages and the randomness of the obtained raw keys and error patterns, standard reconciliation techniques (based, for example, on channel codes) appear to be effective in successfully perform the reconciliation phase between A and B without allowing the eavesdropper to reconstruct the secret key shared by A and B.

More in detail, the talk will report about verification of channel reciprocity in the channel probing phase. A quantization scheme will then be proposed together with a key alignment technique. The proposed

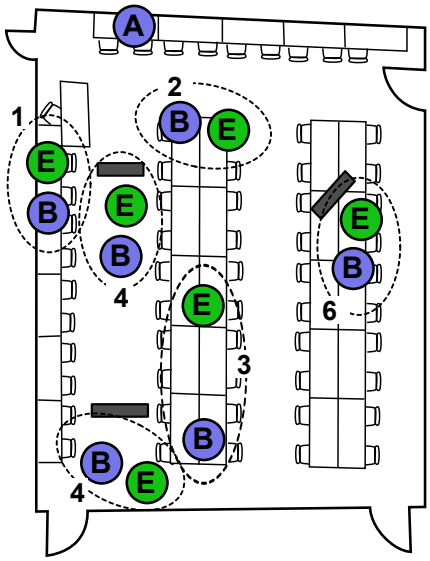

Fig. 1. Floor plan of the laboratory in which waveform acquisition experiments have been carried out. The while the position of Alice was the same for all experiments, the positions of Bob and Eve were changed. Note that cases 1, 2, and 3 correspond to LOS conditions, while cases 4, 5, and 6 to NLOS ones.

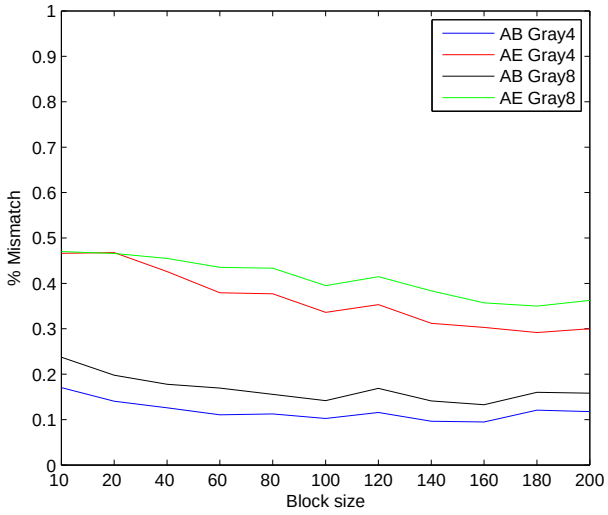

Fig. 2. Percentage of mismatch between Alice-Bob and Alice-Eve raw keys, as a function of the ASBG block size. The result is obtained applying Gray-4 and Gray-8 quantization (LOS propagation).

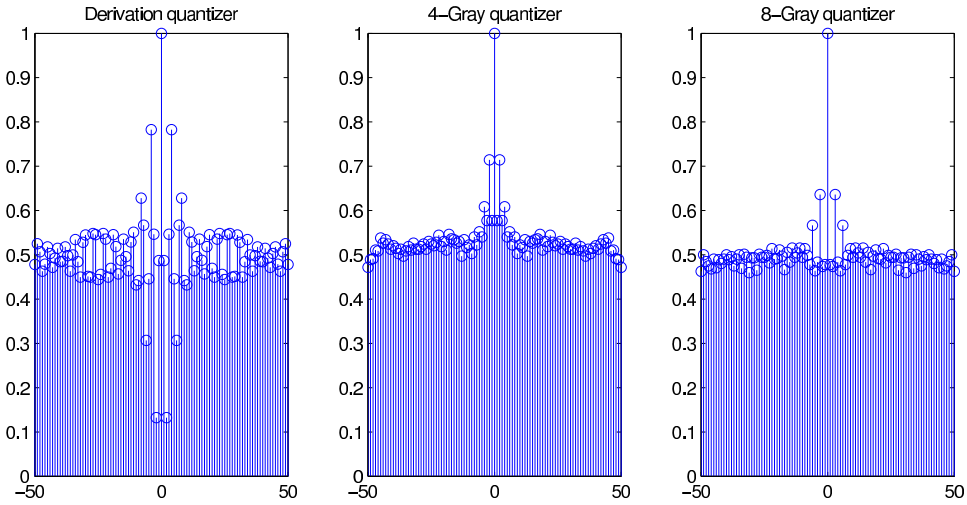

Fig. 3. Autocorrelation function of the raw keys obtained via difference-based, Gray-4, and Gray-8 quantizers. The ASBG block size for Gray-4 and Gray-8 is 20 bits.

scheme, tested with real measurements in an indoor scenario, will be shown to yield raw keys with good randomness properties and tolerable mismatch percentages between Alice and Bob, as well as unfavorable mismatch percentages and random error distribution for Eve.

Figure 1 shows the floor plan of the laboratory in which the measurements have been carried out, along with the different positions of A, B, and E. Figure 2 shows an example of percentages of mismatch measured for the A-B and for the A-E pairs, under different quantization schemes. Figure 3 illustrates the autocorrelation functions for the raw keys obtained with of three different quantizers.