A Stream Ciphering Approach Based on the Wire-Tap Channel Coding

Miodrag J. Mihaljević, Math. Inst. Serbian Academy of Sci.&Arts, Belgrade
Joint work with Hideki Imai

1. Introduction

Usefulness of involvement pure randomness into a cryptographic primitive has been recognized in a number of reported results including the following ones. McEliece public-key system [5] is based on decoding complexity after a noisy channel. Low complexity authentication protocol HB [4] and its improvements (see [2], for example) are based on the problem of solving a system of linear equations corrupted by noise. Particular ideas for employment of a random noise in cryptographic techniques have been reported in [8] as a method to prevent use of the known source statistics by a cryptanalyst. Effects of random noise in certain quantum stream ciphers have been considered in [6].

A different approach for achieving secrecy of communication has been reported in [7] assuming that the channel between the legitimate parties is with a lower noise in comparison with the channel via which a wire-tapper has access to the ciphertext. The method proposed in [7] does not require any secret. It is based on a specific coding scheme which provides a reliably communications within the legitimate parties and prevents, at the same time, the wire-tapper from learning the communication's contents.

On the other hand, according to our best knowledge, up to now there was no one proposal for employment of a pure randomness within a traditional stream cipher. This work originates from a consideration of a possibility to include the noise as a supporting element for achieving the maximum possible security of a stream cipher, i.e. to make it as high as it can be for the employed secret key dimension.

2. Framework of a Novel Paradigm for Stream Ciphers

2.1. **Underlying Ideas.** The main underlying ideas for design of a novel framework for stream ciphers include:

- Encoding/Decoding of the plaintext;
- Encryption/Decryption of the encoded plaintext/ciphertext;
- Wire-tap channel style encoding/decoding of the ciphertext and a deliberate degradation of the codewords before transmission.

Accordingly, the framework of the main operations at the sender's and receiver's sides is as follows:

$$Sender \;:\; Encode \rightarrow Encrypt \rightarrow OutputCipkertextProcessing$$

$$Receiver \;:\; InputCophertextProcessing \rightarrow Decrypt \rightarrow Decode$$

2.2. **Components, Roles and Architecture.** In comparison with a traditional stream cipher which performs "encoding+encryption", the structure of the proposing one has the following three additional components: (i) a source of pure randomness called RAND-box; (ii) a component, which at the encryption side performs encoding of the ciphertext in the dedicated wire-tap channel coding manner and at the decryption side provides the corresponding decoding - we call this component WTCE/WTCD-box (Wire-Tap Channel Encoding/Decoding box); (iii) a component which simulates a pseudorandom binary symmetric channel at the encryption side and performs correction of the pseudorandom errors at the decryption side called PR-box.

Let's call ECC-box a coponent which encodes the plaintext in order to provide correction of the random errors. Note that in the proposing stream cipher ECC-box encodes the plaintext so that it can be recovered correctly after corruption by the errors introduced in the ciphertext deliberately.

Block scheme of the novel stream cipher family is depicted in Fig. 1. The "white" boxes in Fig. 1 correspond to the boxes in a traditional stream cipher which performs "encoding+encryption" in order to perform reliable operation over a noisy communication channel, and the "gray" box are the additional ones.

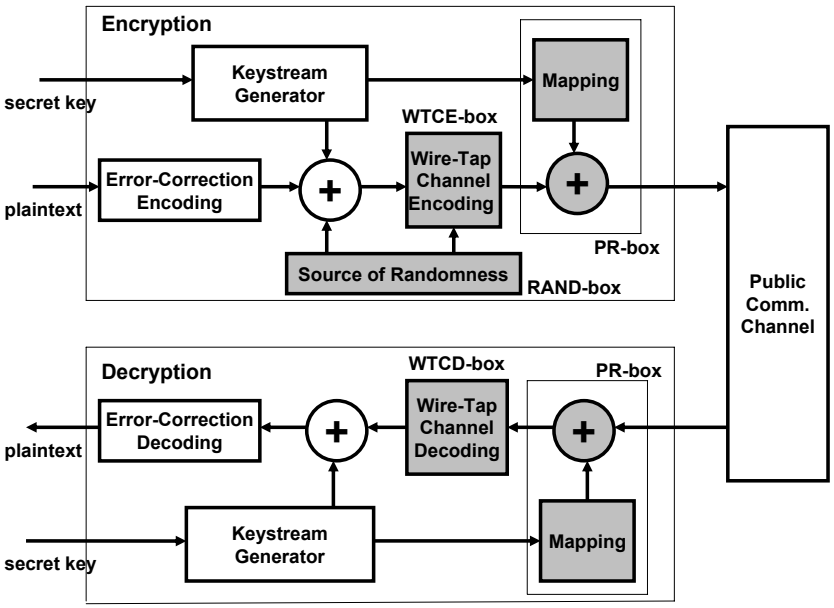

FIGURE 1. Novel stream ciphers framework.

The proposed dedicated wire-tap channel encoding should provide uncertainty about the keystream segments employed for encryption after the PR-box which for an attacker plays role of a binary symmetric channel (BSC) with the crossover probability $p < 1/2$.

Regarding the required characteristics of the dedicated wire-tap channel encoding note the following:

- The WTCE and WTCD should be such that the complexity of theirs implementation is as low as possible. On the other hand, at the same time the complexity of WTCD without the secret key should as high as possible as a consequence of the deliberate pseudorandom degradation of the codewords and should imply a heavy confusion at the attacker's side.
- The proposed paradigm for providing the security is based on the impossibility of WTCD processing without the secret key due to the employed WTCE and the role of PR-box.

Note the following: The main role of the random degradation of the ciphertext before its WTCE is to introduce degradation into a sample which can be available for cryptanalysis preventing a possibility for employment of the generic time-memory trade-off approaches for cryptanalysis (see [3] and [1]) in order to use a generic attacking approach more efficient than the exhaustive search. When an error-free sample is available the time-memory trade-off based attacks can be directly mounted in order to recover the secret key $\mathbf{K}$. On the other hand, when the sample for cryptanalysis is not error-free, the time-memory trade-off approach, in a general case, does not work. The previous statements are consequences of the following. Time-memory trade-off based cryptanalysis is a known plaintext attack technique for cryptanalysis where a sophisticated inversion approach is employed based on an error-free pair of the plaintext and ciphertext. Accordingly, when the

plaintext or ciphertext are not error-free the inversion fails. Particularly note that, in the proposed scheme, without knowledge of the secret key it is not possible to employ error-correction in order to recover error-free plaintext based on its noisy version because in this scenario the plaintext is affected not only by the noise but also by the keystream masking. A similar discussion holds when the time-memory-data trade-off approach, [1], is considered.

The role of the employed homophonic encoding and mapping is to provide a heavy masking of the keystream generator sequences so that they appear as very uncertain for a given ciphertext. Homophonic encoding and the pseudorandom degradation make decoding not feasible without knowledge about the secret key, i.e. the decoding feasibility is equivalent to knowledge of the secret key.

Note that the pseudorandom BSC implies noise only at the attackers side because an attacker does not know the secret key.

3. Concluding Notes

Traditional stream ciphers do not include any randomness: Basically, they are based on the deterministic operations which expand a short secret seed into a long pseudorandom sequence. This paper proposes an alternative approach yielding a novel paradigm for design of stream ciphers.

The proposed framework employs a dedicated coding and a deliberate noise which, assuming the appropriate code and noise level, at the attacker's side provides increased confusion up to the limit determined by the secret key length.

The employed dedicated coding follows the paradigm of the wire-tap channel random encoding, but it is specific: (i) its only purpose is to introduce additional uncertainty at the attackers side, and (ii) decoding complexities with and without the secret key are extremely different.

Security of the proposed stream ciphering has been considered based on the related random model and it is shown that the proposed stream ciphering provides high security which can be as high as indicated by the employed secret key length. The security analysis implies that, under certain conditions, a straightforward exhaustive search over all possible secret keys appears as the most efficient method of cryptanalysis implying that the proposed stream cipher achieves the maximum possible security determined by the secret key length.

In order to achieve the main security goal, the proposed stream ciphering approach includes the following two encoding schemes with impacts on the communications overhead: (i) error-correction encoding of the messages; (ii) dedicated wire-tap channel coding which performs expansion of the initial ciphertext. Both of these issues imply the communications overhead: Accordingly, the proposed stream ciphers framework includes certain trade-off between the security and the communications overhead which in a number of scenarios can be considered as very appropriate.

References

[1] Alex Biryukov and Adi Shamir, *Cryptanalytic time/memory/data tradeoffs for stream ciphers*, ASIACRYPT 2000, Lecture Notes in Computer Science **1976** (2000), 1–13.

[2] Henri Gilbert, Matthew J.B. Robshaw and Yannick Seurin, *HB$^{\#}$: Increasing the Security and Efficiency of HB^{+}*, EUROCRYPT2008, Lecture Notes in Computer Science **4965** (2008), 361–378.

[3] Martin E. Hellman, *A cryptanalytic time-memory trade-off*, IEEE Transactions on Informarmation Theory **26** (1980), 401–406.

[4] Nicholas Hopper and Manuel Blum, *Secure Human Identification Protocols*, ASIACRYPT 2001, Lecture Notes in Computer Science **2248** (2001), 52–66.

[5] Robert J. McEliece, *A public key cryptosystem based on algebraic coding theory*, DSN Progress Report **42–44** (1978), 114–116.

[6] Miodrag J. Mihaljević, *Generic framework for secure Yuen 2000 quantum-encryption employing the wire-tap channel approach*, Physical Review A **75** (2007), 052334–1–5.

[7] Aaron D. Wyner, *The wire-tap channel*, Bell Systems Technical Journal **54** (1975), 1355–1387.

[8] Michael Willett, *Deliberate noise in a modern cryptographic system*, IEEE Transactions on Information Theory **26** (1980), 102–104.