Entropically secure encryption with faster key expansion

Entropically Secure Encryption with Faster Key Expansion

Mehmet Hüseyin Temel and Boris Škorić

Eindhoven University of Technology

m.h.temel@tue.nl, b.skoric@tue.nl

Entropic Security

An encryption scheme is called *perfect* if the ciphertext reveals no information whatsoever about the plaintext. For perfect encryption of *classical* plaintexts the length of the key needs to be at least the entropy of the plaintext, and the simplest cipher is the One-Time Pad (OTP) or Vernam cipher . In the *quantum* setting, perfect encryption of an n-qubit plaintext state requires a key length of $2n$ bits, and the simplest cipher achieving this kind of encryption is the Quantum One-Time Pad (QOTP) [1, 2, 3].

If one does not aim for *perfect* security, it is possible to get information-theoretic guarantees about the encryption even with shorter keys, as long as a lower bound is known on the min-entropy of the plaintext. The notion of (t, ε)-entropic security has been introduced [4, 5], stating that the adversary's advantage in guessing any function of the plaintext is upper bounded by ε if the min-entropy of the plaintext (conditioned on Eve's side information) is at least t. It can be seen as an information-theoretic version of semantic security. It has been shown that (t, ε)-entropically secure encryption of an n (qu)bit plaintext can be achieved with key length $n - t + 2\log\frac{1}{\varepsilon}$ [5, 6, 7]. In the quantum case the t can become negative when Eve's quantum memory is entangled with the plaintext state.

We introduce a new key expansion method for entropically secure encryption, both classical and quantum [8]. The main idea is to *postfix* a pseudorandom string $f(k)$ to the short key k, instead of creating an entirely new string from k. For the computation of $f(k)$ we use finite-field multiplication with a public random string. Our key expansion is faster than previous schemes.

1. The Quantum One-Time Pad

Let $\mathcal{H}_2$ denote the Hilbert space of a qubit. Let Z and X be single-qubit Pauli operators, in the standard basis given by $\left(\begin{smallmatrix}1 & 0\\ 0 & -1\end{smallmatrix}\right)$ and $\left(\begin{smallmatrix}0 & 1\\ 1 & 0\end{smallmatrix}\right)$. The simplest way to encrypt an n-qubit state $\varphi \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$ is to encrypt each qubit independently. The key is $\beta = (\beta_1, \ldots, \beta_n) \in \{0,1\}^{2n}$, with $\beta_i = (s_i, t_i)$.

$$F_\beta(\varphi) = U_\beta \varphi U_\beta^\dagger \quad \text{where } U_\beta = \bigotimes_{i=1}^{n} X^{s_i} Z^{t_i}. \tag{1}$$

If the input state is entangled with the Eve's state i.e. $\varphi^{AE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$, then the effect of QOTP encryption is

$$\varphi^{AE} \quad \mapsto \quad F_\beta(\varphi^{AE}) = (U_\beta \otimes \mathbb{1}^E)\varphi^{AE}(U_\beta^\dagger \otimes \mathbb{1}^E). \tag{2}$$

It holds that $2^{-2n}\sum_{\beta\in\{0,1\}^{2n}} F_\beta(\varphi^{AE}) = \mathbb{1}/2^n \otimes \varphi^E$ for any $\varphi^{AE} \in \mathcal{D}(\mathcal{H}_A \otimes \mathcal{H}_E)$.

2. Entropic Security in the Quantum Setting

Entropic security has been generalized to the fully quantum setting where both the plaintext and ciphertext are quantum states. Desrosiers [6] introduced definitions of entropic security and entropic indistinguishability for quantum ciphers.

Definition: Strong entropic security in the quantum setting (Def.4 in [7]).
An encryption system R is called strongly (t, ε)-entropically secure if for all states $\varphi^{\rm AE}$ satisfying $\mathsf{H}_{\min}(A|E)_\varphi \geq t$, all interpretations $\{(p_i, \sigma_i^{\rm AE})\}$ of $\varphi^{\rm AE}$, all adversaries $\mathcal{A}$ and all functions f, it holds that

$$\left|\Pr[\mathcal{A}(R(\sigma_i^{\rm AE})) = f(i)] - \Pr[\mathcal{A}(R(\varphi^A) \otimes \sigma_i^E) = f(i)]\right| \leq \varepsilon. \tag{3}$$

Here 'interpretation' means $\varphi^{\rm AE} = \sum_i p_i \sigma_i^{\rm AE}$.

Definition: Entropic indistinguishability in the quantum setting (Def.3 in [7]).
An encryption system $R : \mathcal{D}(\mathcal{H}_A) \to \mathcal{D}(\mathcal{H}_{A'})$ is called (t, ε)-indistinguishable if

$$\exists_{\Omega^{A'} \in \mathcal{D}(\mathcal{H}_{A'})} \quad \mathsf{H}_{\min}(A|E)_\varphi \geq t \implies \left\| R(\varphi^{AE}) - \Omega^{A'} \otimes \varphi^E \right\|_1 \leq \varepsilon. \tag{4}$$

Similar to the classical setting, these definitions are equivalent up to parameter changes. **Theorem 1 in [7]**: $(t-1, \varepsilon/2)$-entropic indistinguishability implies strong (t, ε)-entropic security for all functions.
Desrosiers also introduced a scheme with a key length of $n - t + 2\log\frac{1}{\varepsilon}$ using a similar key expansion method as [5]. Here t is the min-entropy of the quantum state. The analysis in [6] applies only if Eve is not entangled with the plaintext. Desrosiers and Dupuis [7] generalized the analysis, with conditional quantum min-entropy as defined by Renner [9], and showed that the results hold even with entanglement. They also proved a minimum required key length of $n - t - 1$.

3. Our scheme

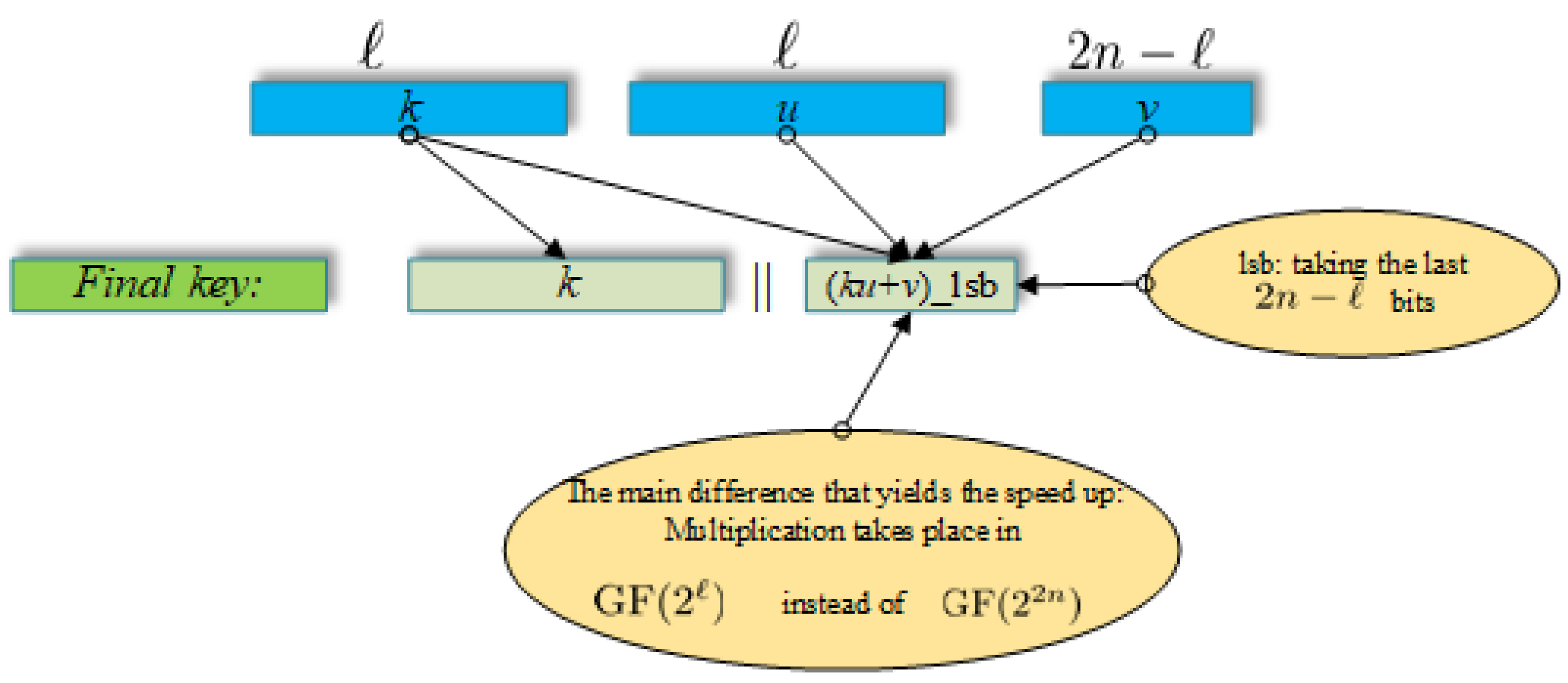
Message state: $\varphi^A \in \mathcal{D}(\mathcal{H}_2^{\otimes n})$

Key: $k \in \{0,1\}^\ell$
The construction shown below is for the case $\ell > n$. The case $\ell < n$ is similar.

Random public strings: $u \in \{0,1\}^\ell$ and $v \in \{0,1\}^{2n-\ell}$

Expanded key: $b(k, u, v) = k \| (uk + v)_{\rm lsb}$

Encryption: $\mathsf{Enc}(k, \varphi^A) = \Big(u, v, F_{b(k,u,v)}(\varphi^A)\Big)$



4. Results

If the key length is set as $\ell = n - t + 2\log\frac{1}{\varepsilon} + 3$ then our scheme is (t, ε)-entropically secure.

- Our key expansion is faster than all previous constructions, while achieving the shortest known key length. In particular, a factor 2 in speed is gained in the unentangled quantum case without further assumptions on Eve.
- The scheme works both for quantum and classical one-time pads.
- Our security proofs are a bit more straightforward.
- We make slightly weaker assumptions on the plaintext, working with collision entropy instead of min-entropy.

References

[1] A. Ambainis, M. Mosca, A. Tapp, and R. de Wolf. Private quantum channels. In *Annual Symposium on Foundations of Computer Science*, pages 547–553, 2000.
[2] P.O. Boykin and V. Roychowdhury. Optimal encryption of quantum bits. *Phys. Rev. A*, 67(4):042317, 2003.
[3] D.W. Leung. Quantum Vernam cipher. *Quantum Information and Computation*, 2(1):14–34, 2002.
[4] A. Russell and H. Wang. How to fool an unbounded adversary with a short key. In *International conference on the theory and applications of cryptographic techniques*, pages 133–148. Springer, 2002.
[5] Y. Dodis and A. Smith. Entropic security and the encryption of high entropy messages. In *Theory of Cryptography Conference*, pages 556–577. Springer, 2005.
[6] S.P. Desrosiers. Entropic security in quantum cryptography. *Quantum Information Processing*, 8(4):331—345, 2009.
[7] S.P. Desrosiers and F. Dupuis. Quantum entropic security and approximate quantum encryption. *IEEE Transactions on Information Theory*, 56(7):3455–3464, 2010.
[8] M. H. Temel and B. Skoric. Approximate quantum encryption with faster key expansion. *arXiv preprint arXiv:2201.00188*, 2022.
[9] R. Renner. Security of quantum key distribution. *International Journal of Quantum Information*, 6(01):1–127, 2008.