Entropoid Based Secret Agreement Scheme

Daniel Nager
daniel.nager@gmail.com

March 2023

Abstract

In this paper we propose a key agreement and its corresponding public key message encryption with a construction based in an entropic operation using circulating matrices described previously in [Gli23].

1 The rings of binary circulant matrices

We will use in this document the circulant matrices and their properties as explained in Gligoroski previous work [Gli23].

As an example we can use $C(863, 2)$, binary circulant matrix sized 863×863, to get 128-bit security.

The main property we're using is the possibility of working with two generated subrings that don't overlap where one is generated with a circulant matrix g, and the second by $T(g)$ where T is the transpose operation, all this under exponentiation of g and $T(g)$.

In both key agreement and public key encryption random secret values must be interpreted as a random exponentiation of such a g as defined in [Gli23].

2 A simple entropic construction

Let's define first a general entropic operation based on a abelian ring G and two commuting automorphism:

$a \bar{*} b = a^e \cdot T(a)^f \cdot b^g \cdot T(b)^h$

The ring is one of the proposed in Section 1, i.e. circulant matrices, and $T(M)$ is the transpose operation on M.

If we define $\lambda_{e,f}(a) = a^e \cdot T(a)^f$, we can prove it's an automorphism:

$\lambda_{e,f}(a \cdot b) = (a \cdot b)^e \cdot T(a \cdot b)^f = a^e \cdot T(a)^f \cdot b^e \cdot T(b)^f = \lambda_{e,f}(a) \cdot \lambda_{e,f}(b)$

and this happens for every e and f exponents.

Furthermore, $\lambda_{e,f}$ and $\lambda_{g,h}$ commute for every e, f, g, h:

$\lambda_{e,f}(\lambda_{g,h}(a)) = (a^g \cdot T(a)^h)^e \cdot T(a^g \cdot T(a)^h)^f = a^{ge} \cdot T(a)^{he} \cdot T(a)^{gf} \cdot a^{hf} = (a^e \cdot T(a)^f)^g \cdot T(a^e \cdot T(a)^f)^h = \lambda_{g,h}(\lambda_{e,f}(a))$

But we can actually apply a simpler formula, so defining the entropic operator as:

$a \overline{*} b = a \cdot b^e \cdot T(b) = r$

Now, the hard problem proposed is with a known e, a and r, find a secret b.

This problem has no apparent relation with the Discrete Logarithm Problem, since the exponent e is known and also the implicit 1 which powers $T(b)$. Also, the circulant matrices of Section 1 ensure it's not possible to relate exponentially b and $T(b)$.

3 Key agreement

Using Section 1 circulant matrices as elements, we profit from the entropic property of $\overline{*}$:

$(C \overline{*} K) \overline{*} (Q \overline{*} C) = (C \overline{*} Q) \overline{*} (K \overline{*} C)$

$\mathcal{A}$ and $\mathcal{B}$ are the two partners involved in the secret agreement. The procedure follows:

$\mathcal{A}$ and $\mathcal{B}$ agree on a constant element C.

$\mathcal{A}$ chooses a secret random K and sends to $\mathcal{B}$ the result of doing $(C \overline{*} K)$.

$\mathcal{B}$ chooses a secret random Q and sends to $\mathcal{A}$ the result of doing $(C \overline{*} Q)$.

$\mathcal{A}$ computes privately $(K \overline{*} C)$ and with $\mathcal{B}$ public value the agreed secret value. This corresponds to the right side of the equality we're profiting.

$\mathcal{B}$ computes privately $(Q \overline{*} C)$ and with $\mathcal{A}$ public value the agreed secret value. This corresponds to the left side of the equality we're profiting.

Both values are the same as $\overline{*}$ is entropic.

In terms of security, let's note that the the role of K and Q is diferent if used as a first or second parameter of $\overline{*}$, in particular, from $(A \overline{*} B)$ cannot be deduced $(B \overline{*} A)$ if B is not known, since we'll need to know B from $B^e \cdot T(B)$.

The considerations about DLP also apply here, so other approaches should be tried, more sophisticated since the analysis of security is actually very simple and clear.

4 Public key encryption

Sending a message to a recipient that publishes it's public key, in this case a known constant C and $P = (C \overline{*} K)$, being K a secret value is done in a similar way as with exponential based key agreements. The sender choose a secret Q and sends to the recipient $R = (C \overline{*} Q)$. With all this information both the sender and the recipient can agree on a shared secret that's used to encrypt the message to be sent.

References

[Gli23] Danilo Gligoroski. *A Transformation for Lifting Discrete Logarithm Based Cryptography to Post-Quantum Cryptography.* Cryptology ePrint Archive, Paper 2023/318. 2023. URL: `https://eprint.iacr.org/2023/318`.