MOVA signature project

Sebastien Duc

1 Overview

We consider a scenario where we have a promoter, which is typically a supermarket chain, and the clients of this chain. The promoter organizes a "game" to which the clients will take part. The game is pretty simple, when a client buys stuff in the supermarket, he wins a certain amount of vouchers depending on how much money he spent. On these vouchers there is a QR-code which has to be scanned by the smartphone of the client. By collecting vouchers, the client can then participate to the daily/weekly/monthly jackpot. Vouchers are associated with a type (i.e. a small picture). Each day/week/month the promoter draws a combination of types of vouchers (i.e. a combination of small pictures). Then if the clients have one of each type that is in the draw, they send it to the promoter using their phone. The N first players to send their vouchers win.

A client can have several vouchers with the same type. But clients are allowed to exchange one of their coupon with other client's coupons.

2 Security

The clients must not be able to forge vouchers. Therefore they are signed by the promoter using MOVA. Because the signatures are of short size, they can be encoded in a QR-code[1]. The vouchers are also provided with a unique identifier to avoid that people use them twice. When a client is sending his combination, he and the promoter can run the batch verification to verify all vouchers in one shot. Since clients can exchange their vouchers, they want to be sure of the authenticity of them when proceeding to the exchange. They can therefore run the verification protocol of MOVA with the promoter to be ensured of the authenticity.

[1] A QR-code can store at most 2953 bytes. So classical signature can also be considered

3 Problems

One problem is when exchanging vouchers, one client can keep a copy of the coupon he is sending.

Another problem is that when verifying for the validity of the vouchers when a client send his combination, it is the promoter that verify if his signatures are valid. Consequently, we may think that some other cryptographic scheme may be more appropriated for this case. The promoter has the secret key so he has the role of the prover in the verification protocol, but he has also the role of the verifier, since he is the one who wants to verify the validity of the signatures. This problem does not arise when verifying during exchange of vouchers between clients.