Cryptanalysis of a Pay-As-You-Watch System

[Published in *Information Processing Letters* **88**(3):119–120, 2003.]

Marc Joye

Gemplus S.A., Card Security Group
La Vigie, Avenue du Jujubier, ZI Athélia IV, 13705 La Ciotat Cedex, France

Abstract. In this paper, we exhibit security flaws in MICROCAST pay-as-you-watch system. From the sole knowledge of public parameters, we show how any intruder is able to forge a coin and so to freely get access to the service.

MICROCAST [2] includes a 'pay-as-you-watch' system for multicast content delivery. In this system, the bank acts as a certification authority. The bank setup goes as follows. Given a randomly chosen 160-bit prime q, two random 512-bit primes p_1 and p_2 are constructed so that q divides $p_1 - 1$. Next, the RSA modulus $n = p_1 p_2$ is formed and a matching pair of RSA public/private exponents (e, d) is computed according to $ed \equiv 1 \pmod{\phi(n)}$. Finally, a generator $g \in (\mathbb{Z}/n\mathbb{Z})^*$ is computed so that the cyclic group $\langle g \rangle$ has order q. The public parameters are n, q, e, and g.

The security of the micropayment system in MICROCAST —that is, the impossibility of coin forgery by an intruder— relies on the difficulty of finding a solution (A, p) to the equation

$$\mathcal{P} A^x \equiv g^p \pmod{n} \tag{1}$$

given $\mathcal{P}$, x, g and n, and where $\mathcal{P}$ is an element of the form $\mathcal{P} = g^\alpha \bmod n$.

In [2, § 4.1], the authors argue that the knowledge of a prime factor of $p_1 - 1$ (namely, q) does not weaken the system. This claim is not justified. Indeed, since p_2 is randomly chosen, it follows, with very high probability, that prime q does not divide $p_2 - 1$. Therefore, from $g^q \equiv 1 \pmod{\{p_1, p_2\}}$, we deduce that $g \equiv 1 \pmod{p_2}$ and so $g \not\equiv 1 \pmod{p_1}$, which yields

$$\gcd(g - 1, n) = p_2 \ .$$

Once the factorization of n is known, it becomes trivial to solve Eq. (1) by computing, for an arbitrary p,

$$A = \left(\frac{g^p}{\mathcal{P}} \right)^{x^{-1} \bmod (p_1 - 1)(p_2 - 1)} \bmod n \ .$$

An easy way that comes to mind for preventing the previous attack consists in choosing prime p_2 such that q divides $p_2 - 1$ and then in constructing g with

order q modulo both p_1 and p_2. But there are other problems. In Eq. (1), as $\mathcal{P}$ is an element of the form $\mathcal{P} = g^\alpha \bmod n$, we have $\mathcal{P}$ —and thus A belong to subgroup $\langle g \rangle \subset (\mathbb{Z}/n\mathbb{Z})^*$. Consequently, even if the factorization of n is unknown, it is still possible to solve Eq. (1) by computing, for an arbitrary p,

$$A = \left(\frac{g^p}{\mathcal{P}}\right)^{x^{-1} \bmod q} \bmod n \ .$$

We further note that keeping secret the value of q does not disallow coin forgery. If generator g has order q modulo both p_1 and p_2 (to avoid the first attack), it follows that q divides both $p_1 - 1$ and $p_2 - 1$. This implies that q divides $p_1 p_2 - 1 = n - 1$ and so it is possible to solve Eq. (1) by computing, for an arbitrary p,

$$A = \left(\frac{g^p}{\mathcal{P}}\right)^{x^{-1} \bmod (n-1)} \bmod n \ .$$

As a conclusion, repairing the micropayment in MICROCAST does not appear straightforward. We invite the reader to investigate new constructions based on the more general representation problem [1].

References

1. S. Brands, "An efficient off-line cash system based on the representation problem," Tech. Report CS-R9323, Centrum voor Wiskunde en Informatica (CWI), April 1993.
2. J. Domingo-Ferrer, A. Martínez-Ballesté, and F. Sebé, "MICROCAST: Smart Card Based (Micro)pay-per-view for Multicast Services," in *Fifth Smart Card Research and Advanced Application Conference (CARDIS '02)*, pp. 125–134, Usenix Association, 2002.