Asymmetric Currency Rounding

[Published in Y. Frankel, Ed., *Financial Cryptography (FC 2000)*, vol. 1962 of *Lecture Notes in Computer Science*, pp. 192–201, Springer-Verlag, 2001.]

David M'Raïhi[1], David Naccache[2], and Michael Tunstall[3]

[1] Gemplus Card International
3 Lagoon Drive, Suite 300, Redwood City, CA 94065, USA
david.mraihi@gemplus.com
[2] Gemplus Card International
34 rue Guynemer, Issy-les-Moulineaux, F-92447, France
david.naccache@gemplus.com
[3] Gemplus Card International
B.P. 100, Gémenos, F-13881, France
michael.tunstall@gemplus.com

Abstract. The euro was introduced on the first of January 1999 as a common currency in fourteen European nations. EC regulations are fundamentally different from usual banking practices for they forbid fees when converting national currencies to euros (fees would otherwise deter users from adopting the euro); this creates a unique fraud context where money can be made by taking advantage of the EC's official rounding rules.

This paper proposes a public-key-based protection against such attacks. In our scheme, the parties conducting a transaction can not predict whether the rounding will cause loss or gain while the expected statistical difference between an amount and its euro-equivalent decreases exponentially as the number of transactions increases.

1 Introduction

Economic and Monetary Union (in short EMU) is a further step in the ongoing process of European integration. EMU will create an area whose economic potential will sustain comparison to that of the United States. Given the size of the euro area, the euro is expected to play an important role as an international currency. As a trade invoicing currency, the euro will also extend its role way beyond direct trade relations.

Issues related to euro conversion were therefore precisely addressed [3] within the general framework of the European financial market. A specific directive stating conversion rules for currencies inside the monetary union was also prepared and issued [1]. The main objective of this directive is to provide financial institutions with a comprehensive set of rules addressing all issues related to currency conversions and currency rounding issues. Although great deal of attention was paid while standardizing the different formulae, the constraint imposed by the requirement of not introducing conversion fees (a political issue) opens the door to new fraud strategies.

In the following sections we explore fraud *scenarii* based on the actual rounding formula and present efficient counter-measures combining randomness and public-key cryptography.

2 Currency Conversion

For centuries, currency conversions have been governed by (rounded) affine functions:

$$f(x) = \text{round}\left(\frac{x}{\rho}\right) - \kappa$$

In financial terms, κ is the banker's *commission* (or *exchange fee*) expressed in the target currency, ρ is the *conversion rate* and the round function is an approximation rule such that for all x:

$$\Delta = \left(\frac{x}{\rho} - f(x)\right) > 0$$

where Δ represents the agent's *benefit* or *margin*.

At the beginning of 1999, the exchange rates between fourteen European currencies have been set with respect to the euro (*cf.* to appendix A) but, being an obstacle to the euro's widespread adoption, exchange fees were forbidden ($\kappa = 0$) by law. EC regulation 1103/97 specifies that the European-wide legally-binding conversion formula is:

$$f(x) = \left\lfloor \frac{x}{\rho} + \frac{1}{2} \right\rfloor$$

This formula can be adjusted for currencies that can be broken up into smaller amounts *e.g.* the British Pound can be broken up into 100 pence. Thus the formula becomes:

$$f(x) = \left\lfloor 100 \times \frac{x}{\rho} + \frac{1}{2} \right\rfloor \times \frac{1}{100}$$

As a characteristic example, the conversion of 1000 FRF into euros would be done as follows:

$$\frac{x_{\text{FRF}}}{\rho_{\text{FRF}}} = \frac{1000}{6.55957} = 152.4490172\ldots \mapsto x_{\text{EUR}} = 152.45\text{EUR}$$

The conversion between two European currencies is somewhat more intricate; the value of the first currency is converted to *scriptural* euros, rounded to three decimal places (*i.e.* 0.1 cent) and then converted into the target currency as illustrated in the next example where 1000 FRF are converted into NLGs:

$$\frac{x_{\text{FRF}}}{\rho_{\text{FRF}}} = \frac{1000}{6.55957} = 152.4490172\ldots \mapsto x_{\text{EUR}} = 152.449\text{EUR}$$

$$x_{\text{EUR}} \times \rho_{\text{NLG}} = 152.449 \times 2.20371 = 335.9533857\ldots \mapsto x_{\text{NLG}} = 335.95\text{NLG}$$

We refer the reader to [1] for further (mainly legal) details.

3 Rounding attacks

Attacks (characterized by a negative Δ) are possible when two different amounts in a given currency collide into the same value in euros; this is only possible when the smallest sub-unit of the concerned currency is worth less than one cent; examples are rather common and easy to construct:

$$\frac{x_{\text{PTE}}}{\rho_{\text{PTE}}} = \frac{1100}{200.482} = 5.48678\ldots \mapsto x_{\text{EUR}} = 5.49\text{EUR}$$

$$\frac{y_{\text{PTE}}}{\rho_{\text{PTE}}} = \frac{1101}{200.482} = 5.49176\ldots \mapsto y_{\text{EUR}} = 5.49\text{EUR}$$

The smallest Portuguese unit is the *centaro* (which only exists for scriptural payments); as the smallest circulating currency unit is the *escudo*, it appears in our example that $x_{\text{EUR}} = y_{\text{EUR}}$ although $x_{\text{PTE}} \neq y_{\text{PTE}}$.

The attacker can therefore create an *escudo ex-nihilo* by investing $x_{\text{PTE}} = 1100$ and converting them to $x_{\text{EUR}} = 5.49$ using the official conversion rule; then, using the EC's formula in the opposite direction, the attacker can convert the x_{EUR} back to *escudos* and cash 1101 PTEs:

$$x_{\text{EUR}} \times \rho_{\text{PTE}} = 5.49 \times 200.482 = 1100.65 \mapsto x'_{\text{PTE}} = 1101\text{PTE}$$

Note that although more decimal places can be used, higher precision neither prevents, nor significantly slows down this potential fraud which becomes particularly relevant when automated attackers (*e.g.* home-based PCs) enter the game.

4 Probabilistic rounding

The most obvious solution to this problem is to charge a minimal amount per transaction, effectively rounding down on every occasion. This solution would be fine for transactions that occur occasionally but not for transactions that occur frequently, especially if the concerned amount is small. The EC have tried to make the Euro as acceptable as possible and introducing a system that rounds down every transaction is more likely to be viewed as a means of making some money rather than preventing possible fraud attacks.

The alternative approach chosen in this paper consists of rounding up with a probability p and down with probability $1-p$, thereby making the rounding unpredictable before completing the conversion process.

At its most simple this would involve rounding with a 1/2 probability as illustrated in the following examples:

$$\begin{tikzcd}
 & x_{\text{EUR}} = 5.49 \text{ EUR} \\
\frac{x_{\text{PTE}}}{\rho_{\text{PTE}}} = \frac{1100}{200.482} = 5.48678\ldots \arrow[ur, "\text{probability } 1/2"] \arrow[dr, "\text{probability } 1/2"'] & \\
 & x_{\text{EUR}} = 5.48 \text{ EUR}
\end{tikzcd}$$

and, repeating the process in the opposite direction:

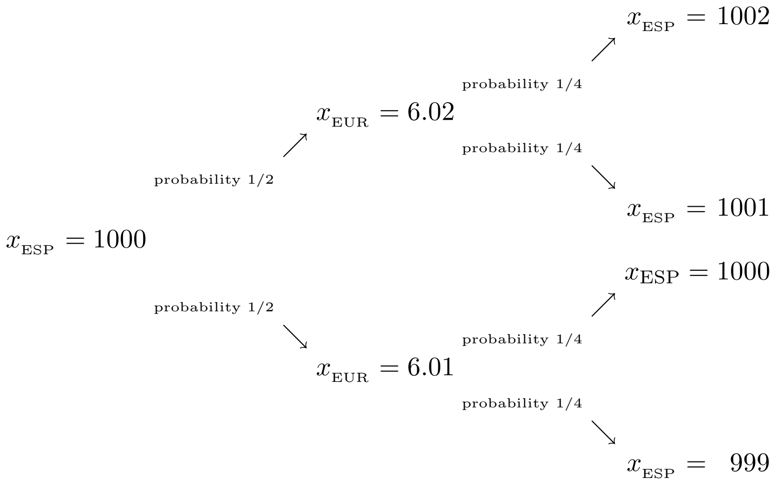
$$\begin{tikzcd}
 & x_{\text{PTE}} = 1101 \text{ PTE} \\
x_{\text{EUR}} \times \rho_{\text{PTE}} = 5.49 \times 200.482 = 1100.65 \arrow[ur, "\text{probability } 1/2"] \arrow[dr, "\text{probability } 1/2"'] & \\
 & x_{\text{PTE}} = 1100 \text{ PTE}
\end{tikzcd}$$

$$\begin{tikzcd}
 & x_{\text{PTE}} = 1099 \text{ PTE} \\
x_{\text{EUR}} \times \rho_{\text{PTE}} = 5.48 \times 200.482 = 1098.64 \arrow[ur, "\text{probability } 1/2"] \arrow[dr, "\text{probability } 1/2"'] & \\
 & x_{\text{PTE}} = 1098 \text{ PTE}
\end{tikzcd}$$

consequently, if numerous transactions are carried out money would be lost as the expected return, $E_{\text{PTE}}(1100)$, is smaller than 1100:

$$E_{\text{PTE}}(1100) = \frac{1101}{4} + \frac{1100}{4} + \frac{1099}{4} + \frac{1098}{4} = 1099.5 < 1100$$

The opposite problem appears when 1000 ESP (where $\rho_{\text{ESP}} = 166.386$) are converted back and forth:



where the expected return is:

$$E_{\text{ESP}}(1000) = \frac{999}{4} + \frac{1000}{4} + \frac{1001}{4} + \frac{1002}{4} = 1000.5 > 1000$$

It is thus possible to take advantage of probabilistic rounding as $p = 1/2$ only slows the attacker by forcing him to expect less return per transaction, but the system's overall behavior remains problematic.

To make x and $E(x)$ equal p should depend on the ratio x/ρ and compensate statistically the rounded digits.

Denoting by $\text{frac}(x) = x - \lfloor x \rfloor$ the fractional part of x, let:

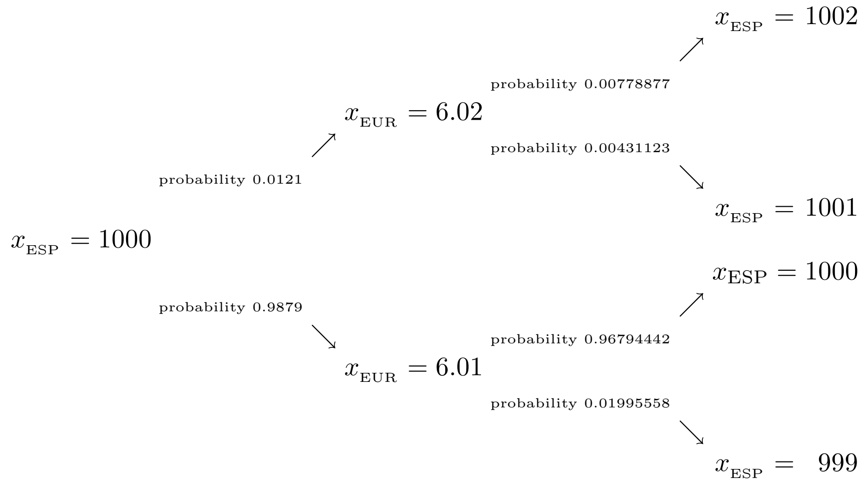
$$p(x, \rho) = \text{frac}\left(100 \times \text{frac}\left(\frac{x}{\rho}\right)\right) \tag{1}$$

be the probability of rounding x currencies at rate ρ.

For example, for 1000 *pesetas* where $x_{\text{ESP}}/\rho_{\text{ESP}} = 6.0101210\ldots$, truncation yields:

$$p(1000, 166.386) = 0.01210\ldots$$

and:



This system has an expected return of:

$$\begin{aligned} E_{\text{ESP}}(1000) &= 0.00778877 \times 1002 + 0.00431123 \times 1001 \\ &\quad 0.96794442 \times 1000 + 0.01995558 \times 999 \\ &= 999.99993319 \cong 1000 \end{aligned}$$

p can be taken to a higher degree of accuracy. If the probabilities are implemented to the highest possible accuracy degree (i.e. all decimal places, where possible), then the expected result will be as close to the value used in the first conversion as possible.

Applied to the previous example the fraud expectation is exactly equal to $1000 + 3 \times 10^{-11}$ ESP. Greater security can only be gained by increasing the accuracy of the exchange rates themselves.

Let x be an amount in a currency whose rate is ρ and denote by $E(x)$ the fraud expectation after a currency ↦ euro probabilistic conversion of x.

We can state the following lemma:

Lemma 1. *Let x be an amount in a currency which rate is ρ and denote by $E(x)$ the fraud expectation after a back and forth (currency ↦ euro ↦ currency) probabilistic conversion of x were $p(x, \rho)$ is determined by formula 1. Then :*

$$E(x) = x$$

Proof :

Denoting by $r(x, \rho)$ the truncation of x/ρ to a two-digit precision :

$$r(x, \rho) = \lfloor \frac{100x}{\rho} \rfloor \times \frac{1}{100},$$

we redefine $p(x, \rho) = (x/\rho - r(x)) \times 100$ and evaluate $E(x)$:

$$\begin{aligned} E(x) &= r(x,\rho) \times (1-p) + (r(x,\rho) + \frac{1}{100}) \times p \\ &= r(x,\rho) + \frac{p}{100} \\ &= r(x,\rho) + \frac{(x/\rho - r(x,\rho)) \times 100}{100} \\ &= r(x,\rho) + x/\rho - r(x,\rho) = x/\rho \end{aligned}$$

and applying the same procedure in the opposite direction we get x back.

Note that since the x/ρ is a rational number, so is the probability $p(x,\rho)$ (say a/b); consequently there is no need to truncate or approximate $p(x,\rho)$, the coin toss can simply consist of picking a random number in the interval $[0, b-1]$ and comparing its value to a.

5 An asymmetric solution

Probabilistic rounding requires an impartial random source $\mathcal{S}$, independent of the interacting parties ($\mathcal{A}$ and $\mathcal{B}$) and (as is usual in cryptography) the best way of generating trust consists of giving neither party the opportunity to deviate from the protocol. The solution is somewhat analogous to [2].

This is hard to achieve with probabilistic rounding, as it is impossible to prove whether x/ρ was rounded correctly or not. Therefore, when $\mathcal{A}$ or $\mathcal{B}$ gains money after a few transactions, it can not be proved if this happened by chance or not. Public-key cryptography can nevertheless serve here, both as $\mathcal{S}$ and as a fair rounding proof.

When a transaction is carried out, transaction data are concatenated and signed by $\mathcal{A}$ and $\mathcal{B}$, using a deterministic signature scheme (typically an RSA [4]). The signatures are then used as randomness source to generate a number $0 \leq \tau \leq 1$ to the same amount of decimal places as the probability $p(x,\rho)$. If $\tau \leq p(x,\rho)$ then the value at the end of the transaction is rounded up, otherwise it is rounded down. Denoting by h a one-way function, the protocol is the following:

- $\mathcal{A}$ and $\mathcal{B}$ negotiate the transaction details t (including the amount to be converted).
- $\mathcal{A}$ sends to $\mathcal{B}$ a sufficiently long (160-bit) random challenge r_A.
- $\mathcal{B}$ sends to $\mathcal{A}$ a sufficiently long (160-bit) random challenge r_B.
- $\mathcal{A}$ and $\mathcal{B}$ sign $h(t, r_A, r_B)$ with their deterministic signature schemes, exchange their signatures (hereafter s_A and s_B) and check their mutual correctness.
- $\tau = s_A \oplus s_B$ is used as explained in the previous section for the rounding operation.

The signatures will convince both parties that once converted, the amount was rounded fairly and prevent $\mathcal{A}$ and $\mathcal{B}$ from perturbing the distribution of τ. Furthermore, the usage of digital signatures permits the resolution of disputes.

Lighter (symmetric) versions of the protocol can be adapted to settings where non-repudiation is not a requirement (*e.g.* the everyday exchange of small amounts) :

- $\mathcal{A}$ and $\mathcal{B}$ generate two sufficiently long random strings r_A and r_B and exchange the hash values $c_A = h(r_A)$ and $c_B = h(r_B)$.
- $\mathcal{A}$ and $\mathcal{B}$ reveal r_A and r_B and check the correctness of c_A and c_B.
- $\tau = r_A \oplus r_B$ is used for the rounding operation.

Finally, note that (as most two-party symmetric e-cash protocols) our symmetric variant is vulnerable to protocol interrupt attacks. Such attacks consist in abandoning a transaction (*e.g.* walk out of the shop) if the rounding does not happen to be in favor of the abandoning party.

6 Conclusion

This paper presented a counter-measure that prevents a fraud scenario inherent to EC regulation 1103/97. Although current regulations do not present serious problems when applied occasionally in coin and bank-note conversions, the procedures proposed in this paper is definitely preferable in large-scale electronic fund transfers where automated attacks could cause significant losses.

7 Acknowledgments and further references

We would like to thank the anonymous referees for their useful remarks, George Davida and Yair Frankel for their kind and helpful support.

The authors would like to out that after the presentation of this paper, Ron Rivest mentioned that the probabilistic rounding idea appears in his FC'97 rumps session lottery protocol (see [5] as well).

References

1. Council Regulation (EC) No 1103/97 of June 17-th 1997 on certain provisions relating to the introduction of the euro.
2. M. Blum, *Coin flipping by telephone: a protocol for solving impossible problems*, 24-th IEEE Spring computer conference, IEEE Press, pp. 133–137, 1982.
3. DGII/D1 (EC), Note II/717/97-EN-Final, *The introduction of the euro and the rounding of currency amounts*, 1997.
4. R. Rivest, A. Shamir and L. Adleman, *A method for obtaining digital signatures and public-key cryptosystems*, CACM, vol. 21, no. 2, pp. 120–126, 1978.
5. D. Wheeler, *Transactions Using Bets*, Security protocols workshop 1996, Lecure Notes in Computer Science no. 1189, Springer-Verlag, 1997.

A Euro Exchange Rates

country	**symbol**	**currency**	ρ =**currency/euro**
Austria	ATS	schilling	13.7603
Belgium	BEC	franc	40.3399
Denmark	DKK	krona	7.43266
Finland	FIM	mark	5.94575
France	FRF	franc	6.55956
Germany	DEM	mark	1.95587
Greece	GRD	drachma	326.300
Ireland	IEP	punt	0.78786
Italy	ITL	lira	1936.27
Luxemburg	LUF	franc	40.3399
Netherlands	NLG	guild	2.20374
Portugal	PTE	escudo	200.481
Spain	ESP	peseta	166.388
Sweden	SEK	krona	8.71925

B EC Regulation 1103/97

Article 4.

1. *The conversion rates shall be adopted as one euro expressed in terms of each of the national currencies of the participating Member States. They shall be adopted with six significant figures.*
2. *The conversion rates shall not be rounded or truncated when making conversions.*
3. *The conversion rates shall be used for conversions either way between the euro unit and the national currency units. Inverse rates derived from the conversion rates shall not be used.*
4. *Monetary amounts to be converted from one national currency unit into another shall first be converted into a monetary amount expressed in the euro unit, which amount may be rounded to not less than three decimals and shall then be converted into other national currency unit. No alternative method of calculation may be used unless it produces the same results.*

Article 5.

Monetary amounts to be paid or accounted for when a rounding takes place after a conversion into the euro unit pursuant to Article 4 shall be rounded up or down to the nearest cent. Monetary amounts to be paid or accounted for which are converted into a national currency unit shall be rounded up or down to the nearest sub-unit or in the absence of a sub-unit to the nearest unit, or according to national law or practice to a multiple or fraction of the sub-unit or unit of the national currency unit. If the application of the conversion rate gives a result which is exactly half-way, the sum shall be rounded up.