







formules d'addition et de doublement. La formule calculant le paramètre  $\lambda$  dans le cas  $P_1 \neq \pm P_2$  (cf. section 2) ne peut pas être utilisée pour le doublement car dans ce cas  $x_1 = x_2$ , et le dénominateur de  $\lambda$  s'annule. Brier *et al.* ont utilisé une série de manipulations algébriques afin d'obtenir une formulation de  $\lambda$  qui est définie à la fois pour l'addition et le doublement [9]. Dans le cas où la caractéristique du corps fini  $\mathbb{K}$  est différente de 2 ou de 3, et si  $y_1 + y_2 \neq 0$ ,  $\lambda$  peut être écrit sous la forme :

$$\lambda = \frac{(x_1 + x_2)^2 - x_1x_2 + a_4}{y_1 + y_2}$$

On peut remarquer que cette formulation contient une faiblesse intrinsèque : lorsque  $y_1 + y_2 = 0$ ,  $\lambda = O$ . Izu *et al.* ont montré que, sous certaines conditions, cette faiblesse peut permettre de retrouver la clé [10].

Pour pallier à ce problème, Déchène *et al.* ont développé une famille de formules unifiées d'addition de points qui sont définies pour toutes les valeurs possibles des coordonnées de points [11]. Parmi toute cette famille, celle induisant le moins de calculs intermédiaires s'écrit, lorsque  $y_1 + y_2 + (-1)^\delta(x_1 - x_2) \neq 0$  :

$$\lambda = \frac{(x_1 + x_2)^2 - x_1x_2 + a_4 + (-1)^\delta(y_1 - y_2)}{y_1 + y_2 + (-1)^\delta(x_1 - x_2)}$$

avec, lorsque  $y_1 + y_2 + x_1 - x_2 \neq 0$ ,  $\delta = 0$ , sinon  $\delta = 1$ .

## 5. Conclusion

Protéger un cryptosystème contre un certain type d'attaque peut le rendre plus vulnérable face à un autre type d'attaque. Ce concept a été illustré dans cet article par la protection de la multiplication scalaire des courbes elliptiques face aux attaques par analyse de canaux cachés : le remplacement de l'algorithme *double-and-add* par l'algorithme *double-and-add-always* rend le dispositif vulnérable face aux attaques de type *safe-error*. De même, les formules unifiées d'addition et de doublement ne doivent pas amener de failles mathématiques exploitables : celles proposées dans [9] en contenaient une utilisable par les attaquants.

De plus, l'amélioration des performances d'un cryptosystème va parfois de pair avec une fragilisation de celui-ci. Par exemple, l'utilisation d'une technique de recodage de la clé appelée *wNAF* diminue le nombre global d'opérations à effectuer lors de la multiplication scalaire, mais peut faciliter une attaque de type *sign-change fault attack* [12].

Les futurs travaux consisteront à trouver de nouveaux opérateurs arithmétiques pour courbes elliptiques résistants à la fois aux attaques par analyse de canaux cachés et aux attaques en fautes. Une unité arithmétique est en cours d'implémentation : la prochaine étape sera de la sécuriser, tout en conservant un haut niveau de performance.

**Remerciements.** Ce travail fait l'objet d'un thèse à financement Fonds Social Européen (FSE) dans le cadre du projet BTRS (Briques Technologiques pour le Renforcement de la Sécurité), dont les partenaires industriels

sont Gemalto et SPS. Le laboratoire SESAM est une équipe mixte CEA-LETI/École Nationale Supérieure des Mines de Saint-Étienne, basée sur le site Georges Charpak de Gardanne.

Les auteurs remercient Arnaud Tisserand et Jean-Claude Bajard (LIRMM, Équipe ARITH, CNRS) pour leurs relectures.

## Références

- [1] V. Miller. Use of Elliptic Curve in Cryptography. In *Advances in Cryptology – CRYPTO, LNCS*, volume 218, pages 417–426, 1986.
- [2] N. Koblitz. Elliptic Curve Cryptosystems. *Mathematics of Computation*, 48(177) :203–209, 1987.
- [3] P. Kocher. Timing Attacks on Implementations of Diffie-Hellman, RSA, DSS, and other Systems. In *Advances in Cryptology – CRYPTO, LNCS*, volume 1109, pages 104–113, 1996.
- [4] P. Kocher, J. Jaffe, and B. Jun. Differential Power Analysis. In *Advances in Cryptology – CRYPTO, LNCS*, volume 1666, pages 388–397, 1999.
- [5] K. Gandolfi, C. Moutrel, and F. Olivier. Electro-magnetic Analysis : Concrete Results. In *Proc. Cryptographic Hardware and Embedded Systems – CHES, LNCS*, volume 2162, pages 251–261, 2001.
- [6] S.P. Skorobogatov and R.J. Anderson. Optical Fault Induction Attacks. In *Proc. Cryptographic Hardware and Embedded Systems – CHES, LNCS*, volume 2523, pages 2–12, 2002.
- [7] J.-S. Coron. Resistance against Differential Power Analysis for Elliptic Curve Cryptosystem. In *Proc. Cryptographic Hardware and Embedded Systems – CHES, LNCS*, volume 1717, pages 292–302, 1999.
- [8] S.-M. Yen and M. Joye. Checking before Output May not be Enough against Fault-Based Cryptanalysis. *IEEE Transactions on Computers*, 49(9) :967–970, 2000.
- [9] É. Brier and M. Joye. Weierstrass Elliptic Curves and Side-Channel Attacks. In *Proc. Public Key Cryptography – PKC, LNCS*, volume 2274, pages 335–345, 2002.
- [10] T. Izu and T. Takagi. Exceptional Procedure Attack on Elliptic Curve Cryptosystems. In *Proc. Public Key Cryptography – PKC, LNCS*, volume 2567, pages 224–239, 2003.
- [11] I. Déchène, É. Brier, and M. Joye. Unified Point Addition Formulae for Elliptic Curve Cryptosystems. In *Embedded Cryptographic Hardware : Methodologies and Architectures – Nova Science Publishers*, pages 247–256, 2004.
- [12] J. Blömer, M. Otto, and J.-P. Seifert. Sign Change Fault Attacks on Elliptic Curve Cryptosystems. In *Proc. Fault Diagnosis and Tolerance in Cryptography – FDTCT, LNCS*, volume 4236, pages 36–52, 2006.