Système de chiffrement pour GSM : A5 family
Cracking via GPU

Gloire, Gwendal
Project Kalkulator's Knights

Hackito Ergo Sum 2010

Sommaire

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x01 L'histoire

- La téléphonie mobile numérique débute réellement en 1982.

--Le groupe « GSM » est crée par la « CEPT »

|

|__ élaboration des normes

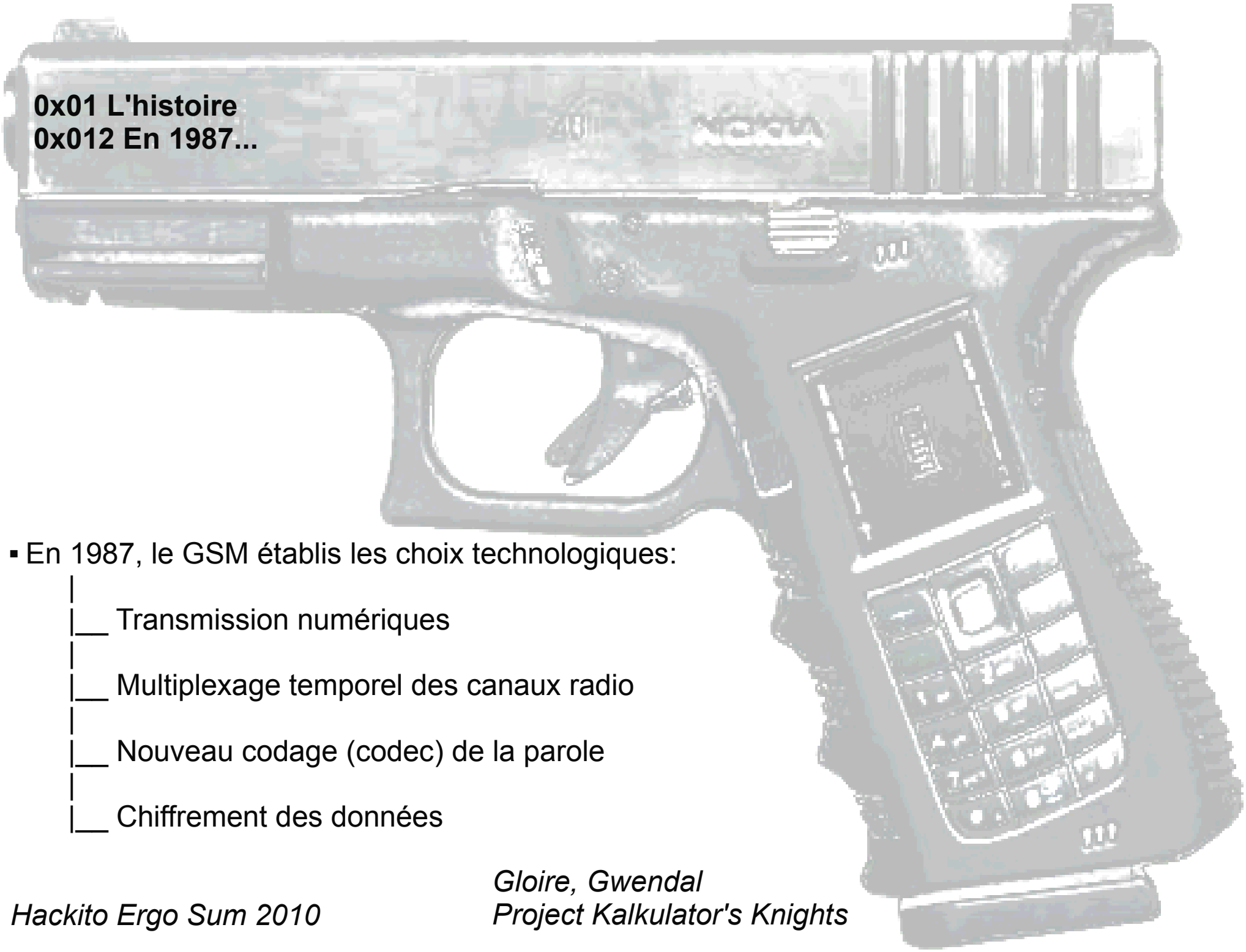
0x01 L'histoire
0x011 Dans les années 80...

- Dans les années 80, on assiste au développement numérique dans le domaine des transmissions et le traitement des signaux
  - |
  - |__ Techniques de transmission fiables

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x01 L'histoire
0x012 En 1987...

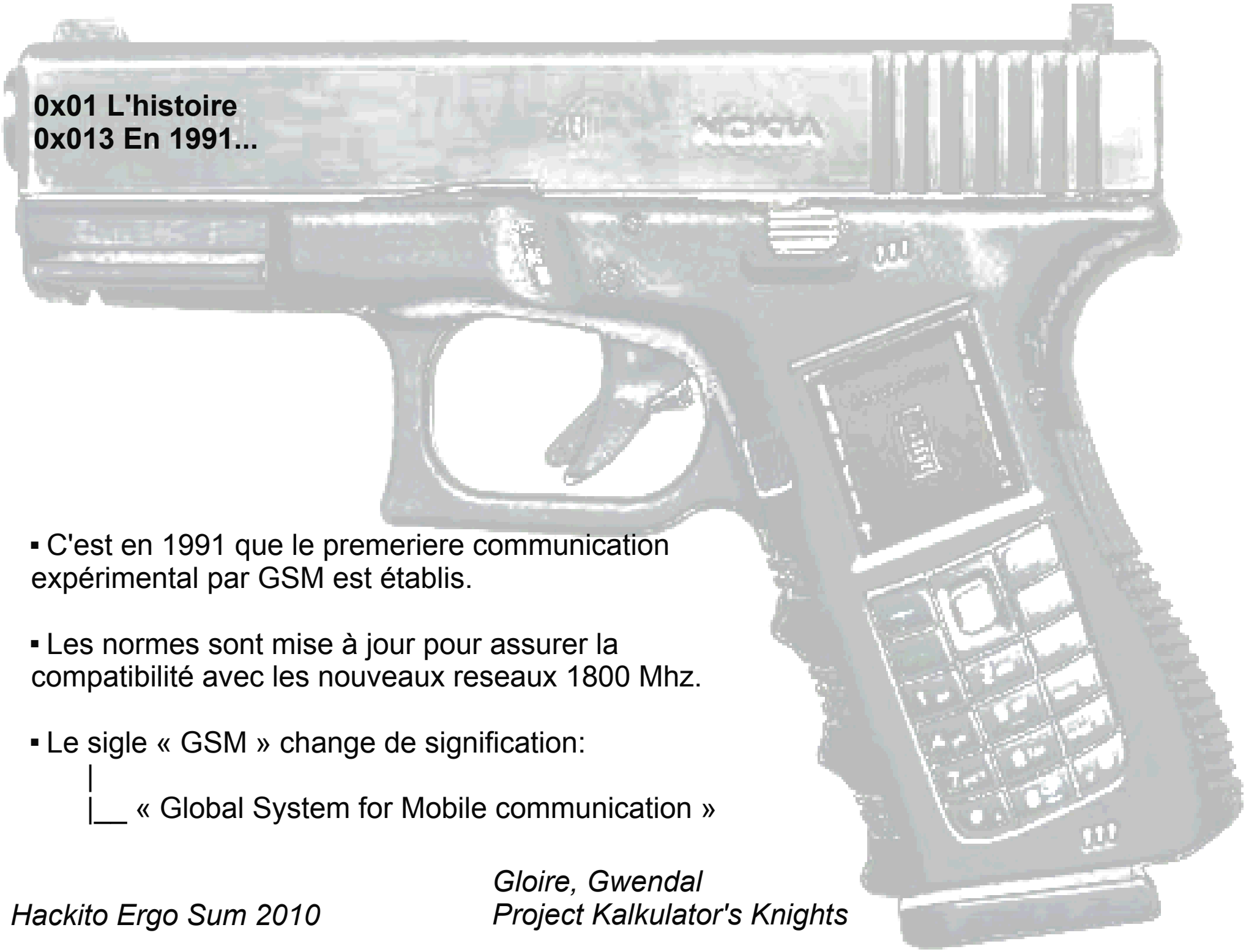


- En 1987, le GSM établis les choix technologiques:
  - Transmission numériques
  - Multiplexage temporel des canaux radio
  - Nouveau codage (codec) de la parole
  - Chiffrement des données

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x01 L'histoire
0x013 En 1991...



- C'est en 1991 que le premeriere communication expérimental par GSM est établis.

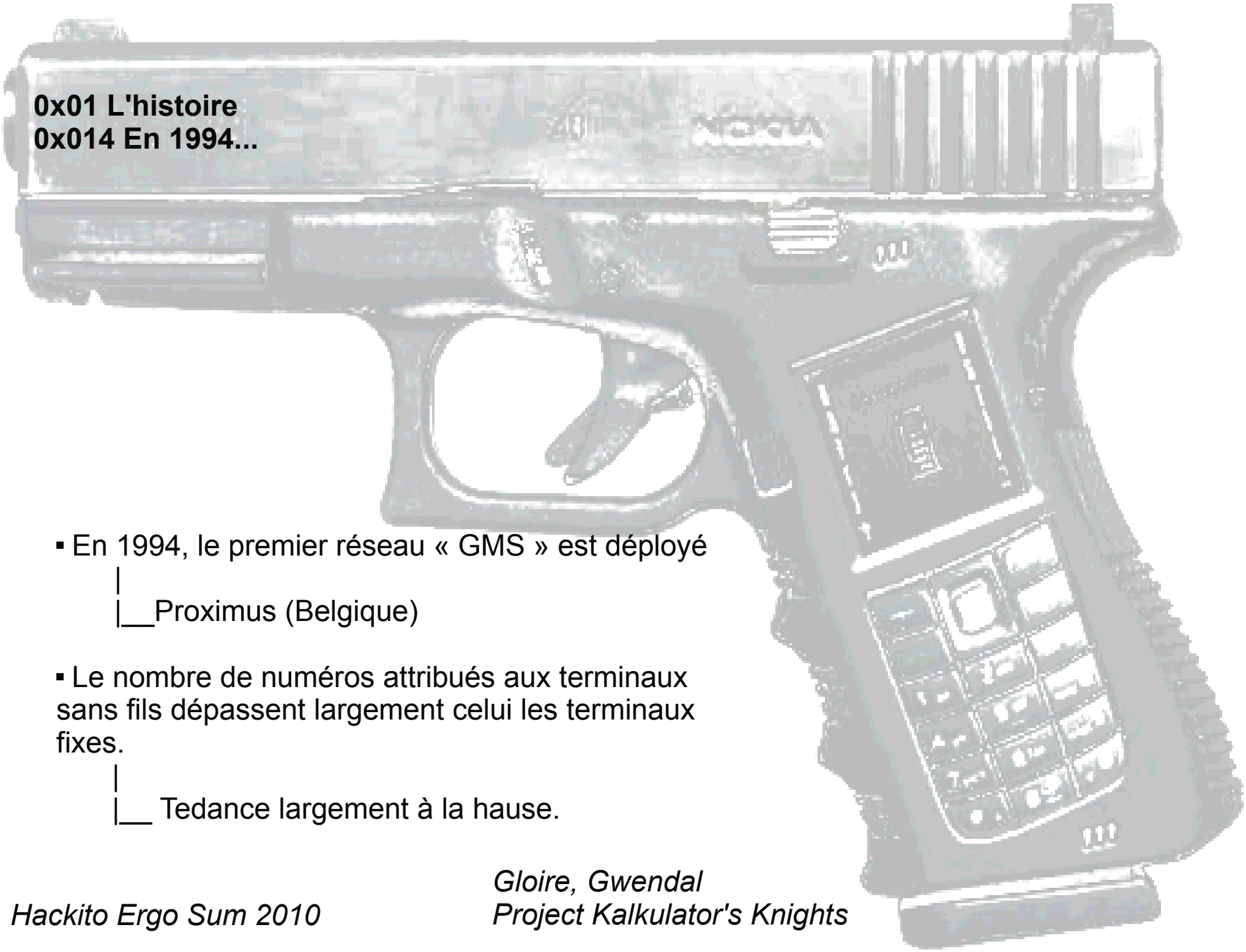
- Les normes sont mise à jour pour assurer la compatibilité avec les nouveaux reseaux 1800 Mhz.

- Le sigle « GSM » change de signification:
  |
  |__ « Global System for Mobile communication »

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x01 L'histoire
0x014 En 1994...



- En 1994, le premier réseau « GMS » est déployé
  |
  |__Proximus (Belgique)

- Le nombre de numéros attribués aux terminaux sans fils dépassent largement celui les terminaux fixes.
  |
  |__ Tedance largement à la hause.

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x01 L'histoire
0x015 Frise chronologique

A B C D

A 1982 Début de la téléphonie numérique
B 1987 Définition des spécifications
C 1991 Première communication expérimental GSM
D 1994 Premier réseau GSM déployé en Belgique

Hackito Ergo Sum 2010

Gloire Gwendal
Project Kalkulator's Knights

0x02 Le fonctionnement

A5

Terminal

Antenne relais

Gloire, Gwendal
Project Kalkulator's Knights

0x02 Le fonctionnement
0x021 La famille A5

A5/1 Chiffrement standard
A5/2 Chiffrement « export »
A5/3 Mécanisme d'authentification

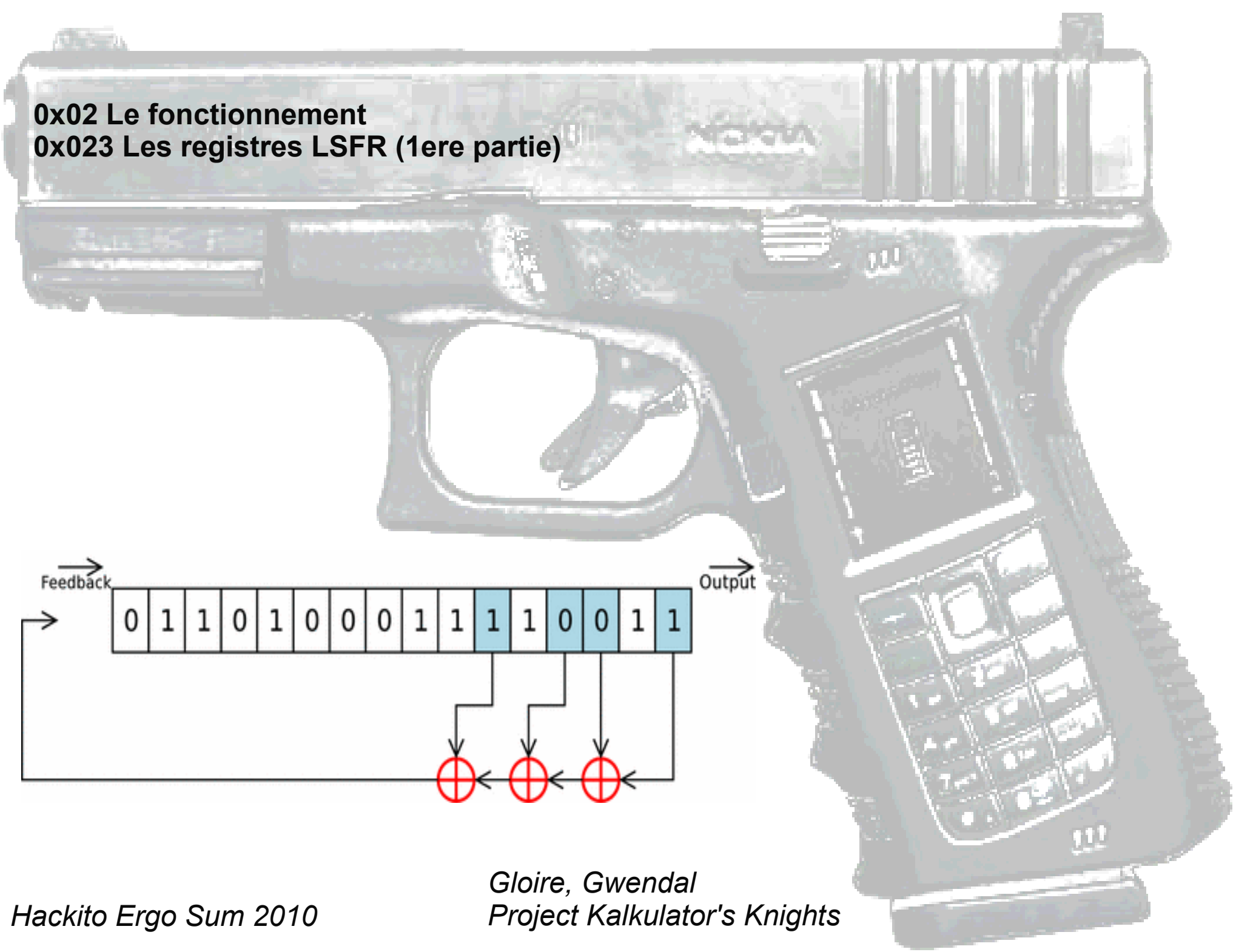
Gloire, Gwendal
Project Kalkulator's Knights

Hackito Ergo Sum 2010

0x02 Le fonctionnement
0x022 Les spécifications du A5/1

- Algorithme de chiffrement par flot
- Initialiser par une clé de 64 bits
- 3 registres a décalage LSFR

Gloire, Gwendal
Project Kalkulator's Knights

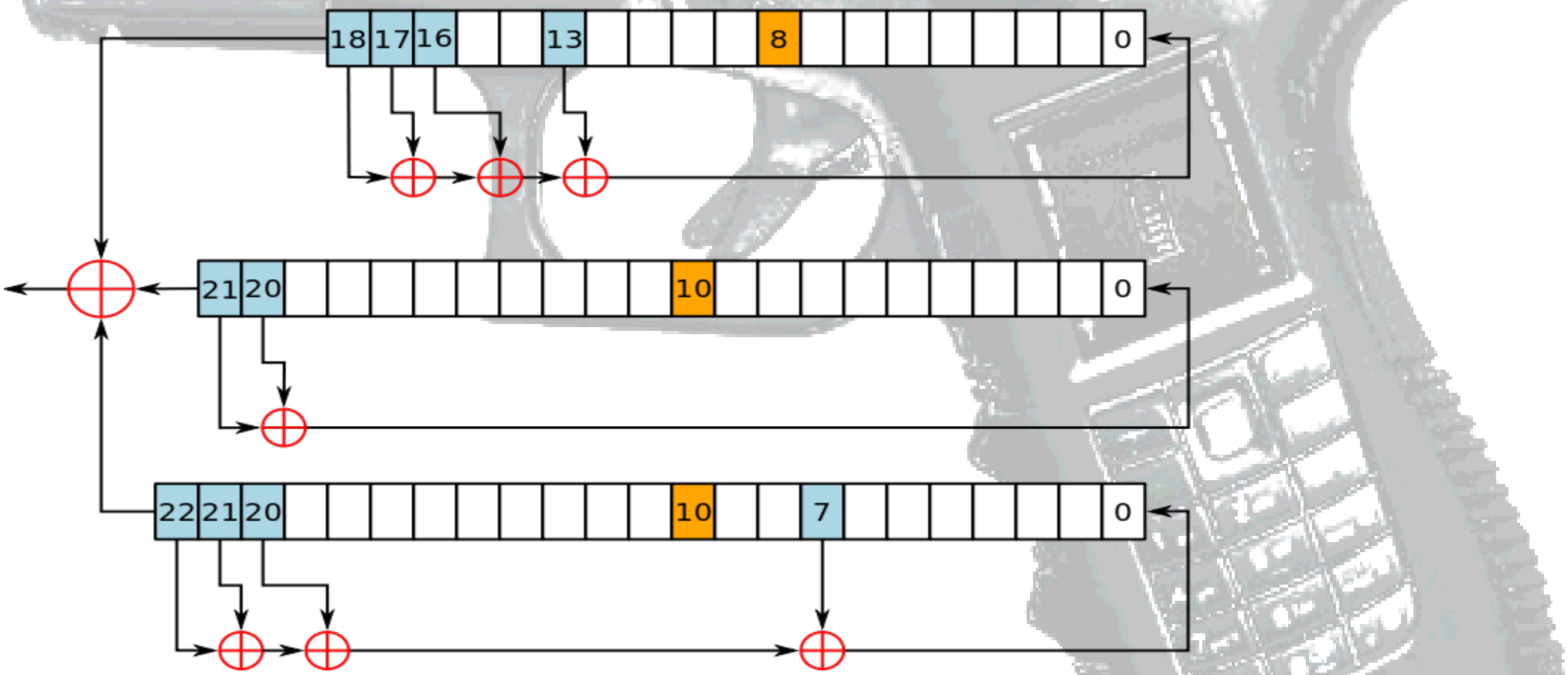


0x02 Le fonctionnement
0x023 Les registres LSFR (1ere partie)

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x02 Le fonctionnement
0x024 Les registres LSFR (2eme partie)



Gloire, Gwendal
Project Kalkulator's Knights

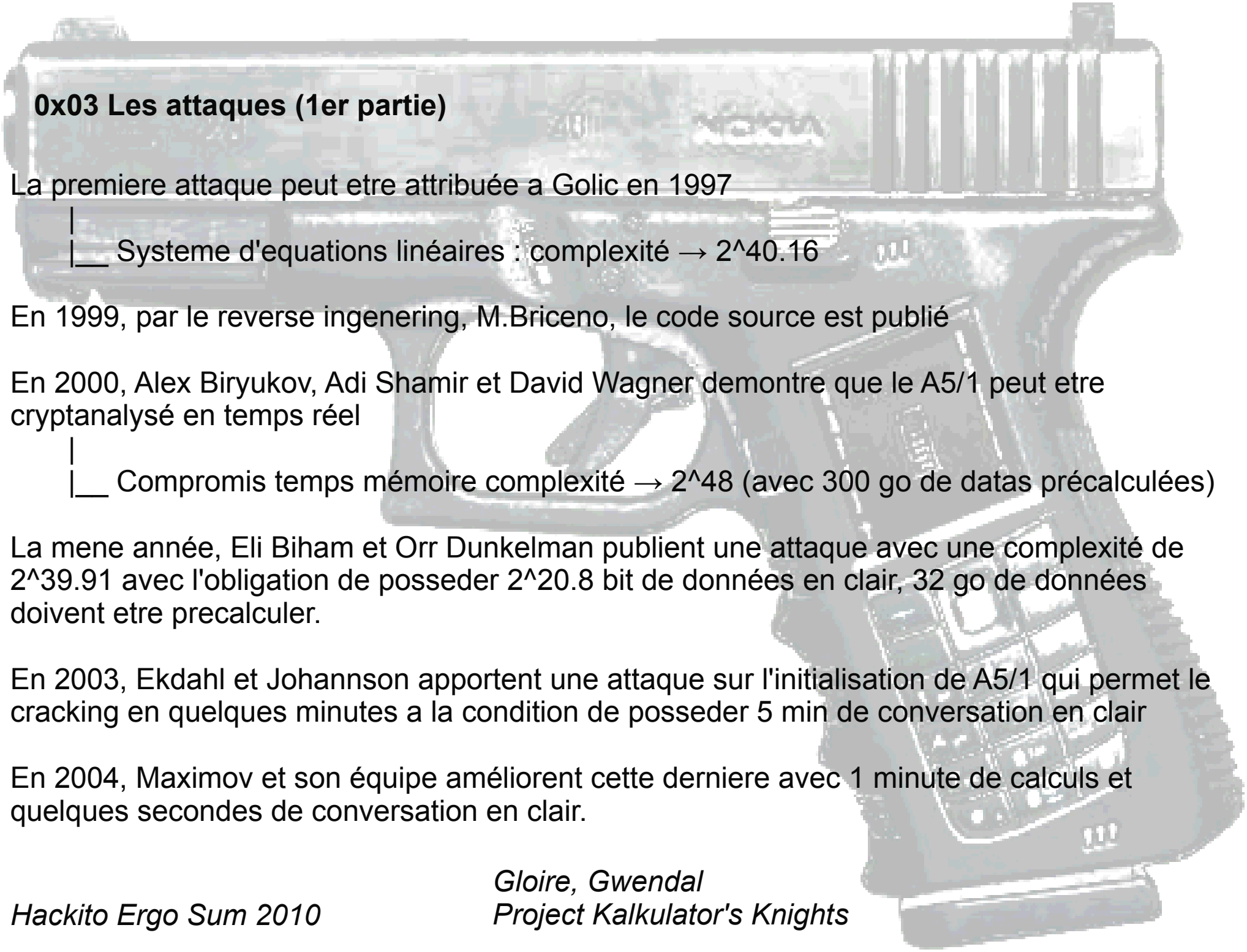
0x02 Le fonctionnement
0x025 Fonctionnement des registres

T1 → Initialisation des 3 registres en les mettant à zéro

T2 → 64 cycles pendant lequel la clé K est introduite

T3 → Décalage des registres

Gloire, Gwendal
Project Kalkulator's Knights



0x03 Les attaques (1er partie)

La premiere attaque peut etre attribuée a Golic en 1997
|
|__ Systeme d'equations linéaires : complexité → 2^40.16

En 1999, par le reverse ingenering, M.Briceno, le code source est publié

En 2000, Alex Biryukov, Adi Shamir et David Wagner demontre que le A5/1 peut etre cryptanalysé en temps réel
|
|__ Compromis temps mémoire complexité → 2^48 (avec 300 go de datas précalculées)

La mene année, Eli Biham et Orr Dunkelman publient une attaque avec une complexité de 2^39.91 avec l'obligation de posseder 2^20.8 bit de données en clair, 32 go de données doivent etre precalculer.

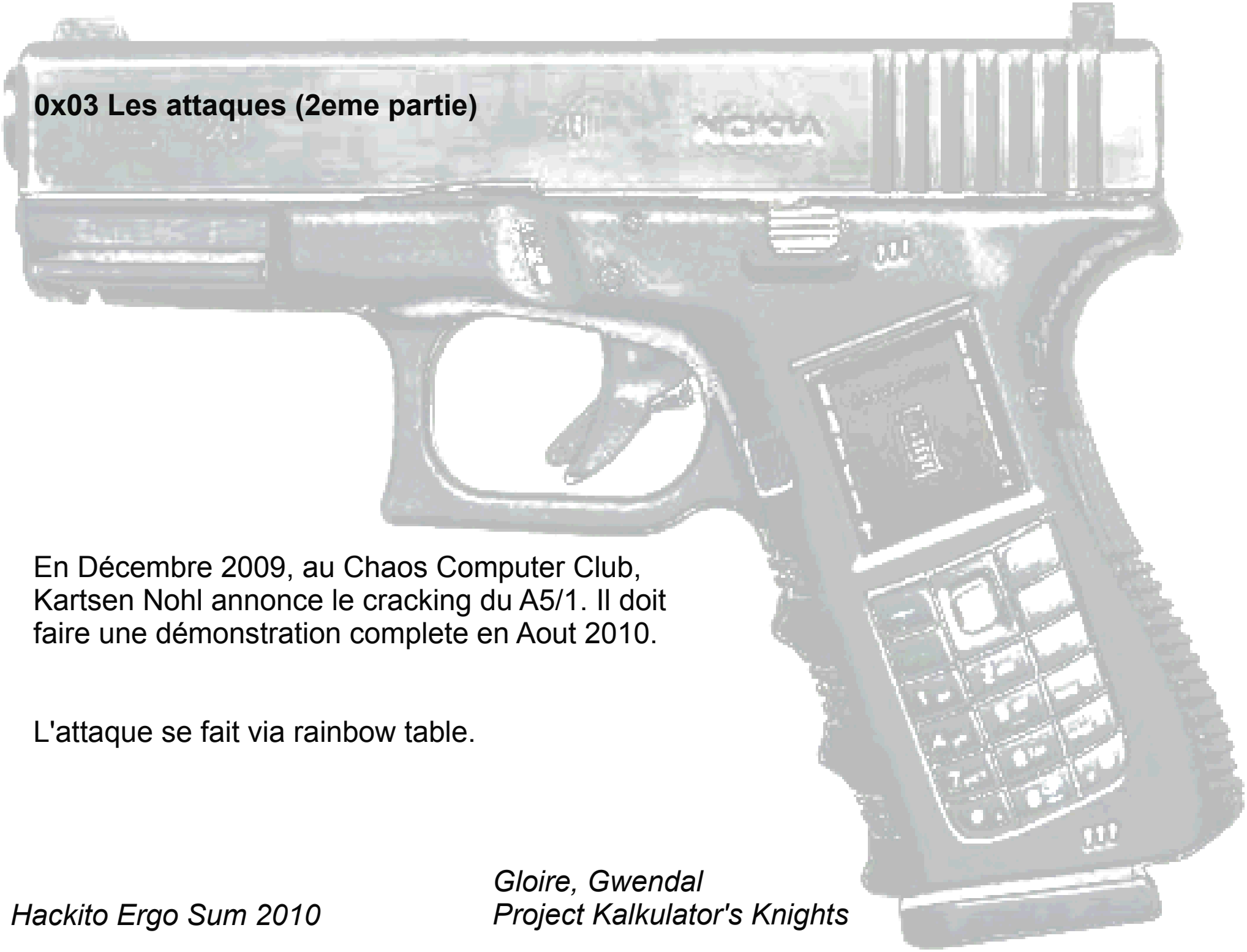
En 2003, Ekdahl et Johannson apportent une attaque sur l'initialisation de A5/1 qui permet le cracking en quelques minutes a la condition de posseder 5 min de conversation en clair

En 2004, Maximov et son équipe améliorent cette derniere avec 1 minute de calculs et quelques secondes de conversation en clair.

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x03 Les attaques (2eme partie)



En Décembre 2009, au Chaos Computer Club, Kartsen Nohl annonce le cracking du A5/1. Il doit faire une démonstration complete en Aout 2010.

L'attaque se fait via rainbow table.

Hackito Ergo Sum 2010

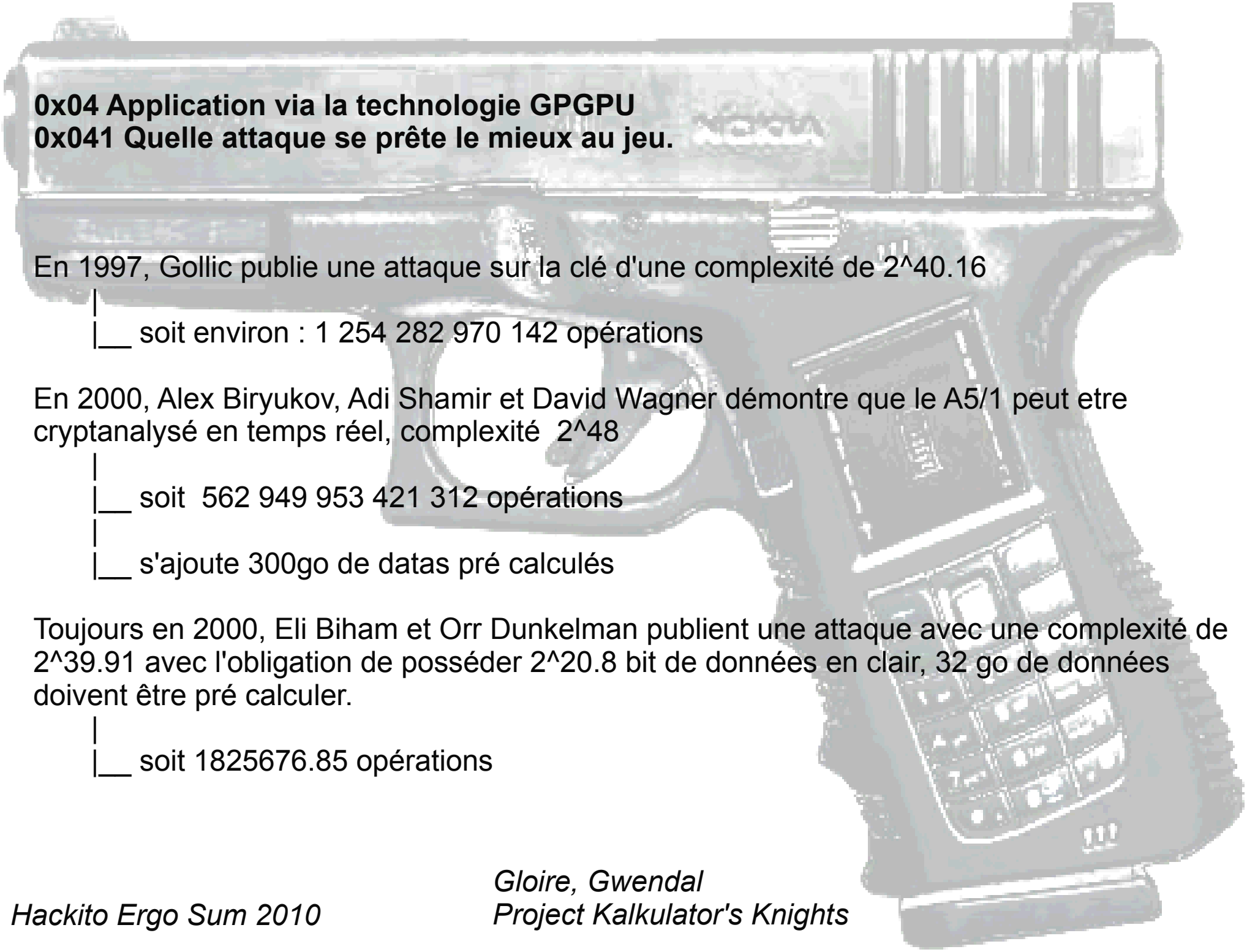
Gloire, Gwendal
Project Kalkulator's Knights

0x04 Application via la technologie GPGPU

Le A5/1 est un algorithme de chiffrement dit fort.
|
|__ de nombreux calculs.

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights



0x04 Application via la technologie GPGPU
0x041 Quelle attaque se prête le mieux au jeu.

En 1997, Gollic publie une attaque sur la clé d'une complexité de 2^40.16

|
|__ soit environ : 1 254 282 970 142 opérations

En 2000, Alex Biryukov, Adi Shamir et David Wagner démontre que le A5/1 peut etre cryptanalysé en temps réel, complexité 2^48

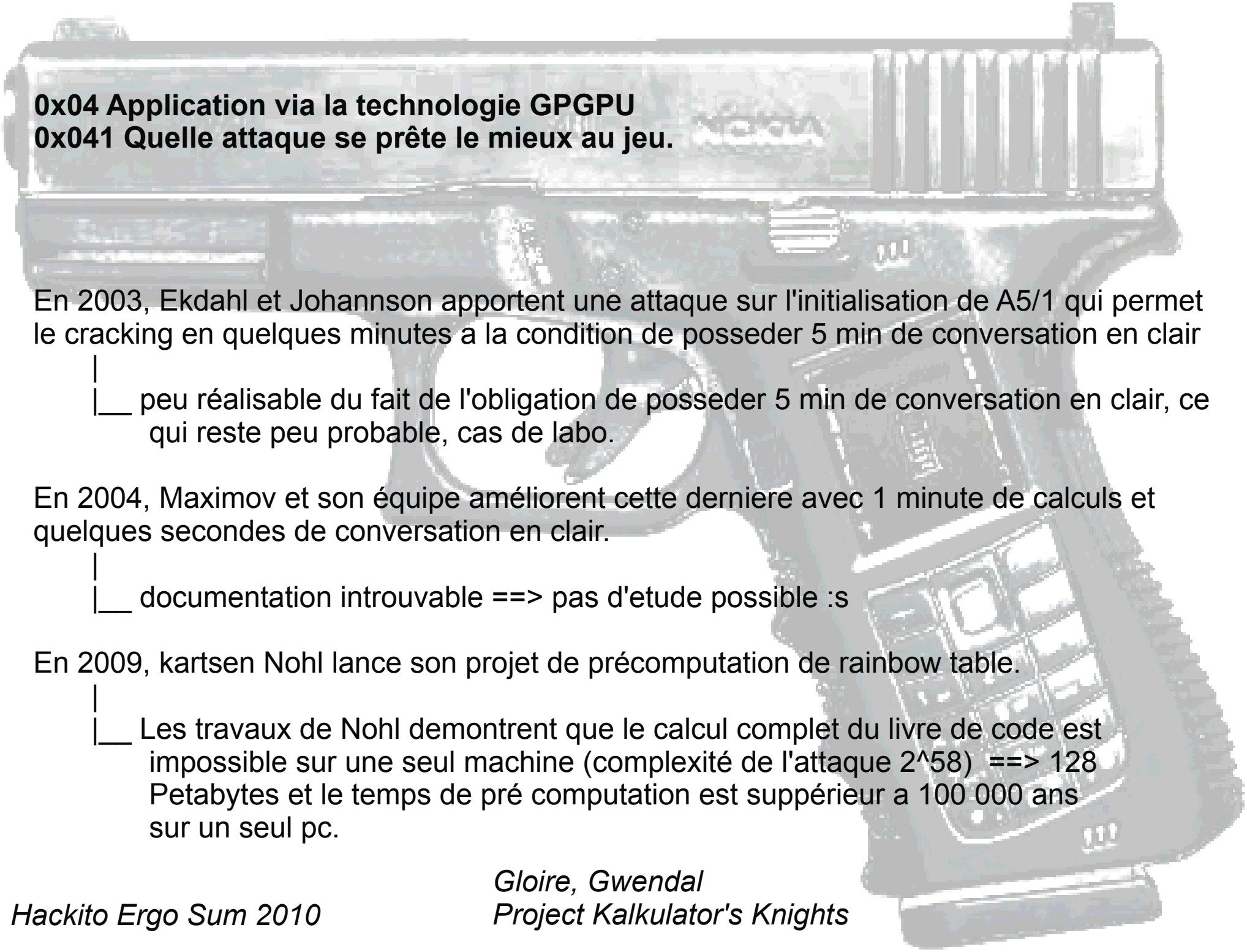
|
|__ soit 562 949 953 421 312 opérations
|
|__ s'ajoute 300go de datas pré calculés

Toujours en 2000, Eli Biham et Orr Dunkelman publient une attaque avec une complexité de 2^39.91 avec l'obligation de posséder 2^20.8 bit de données en clair, 32 go de données doivent être pré calculer.

|
|__ soit 1825676.85 opérations

Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights



0x04 Application via la technologie GPGPU
0x041 Quelle attaque se prête le mieux au jeu.

En 2003, Ekdahl et Johannson apportent une attaque sur l'initialisation de A5/1 qui permet le cracking en quelques minutes a la condition de posseder 5 min de conversation en clair

|
|__ peu réalisable du fait de l'obligation de posseder 5 min de conversation en clair, ce qui reste peu probable, cas de labo.

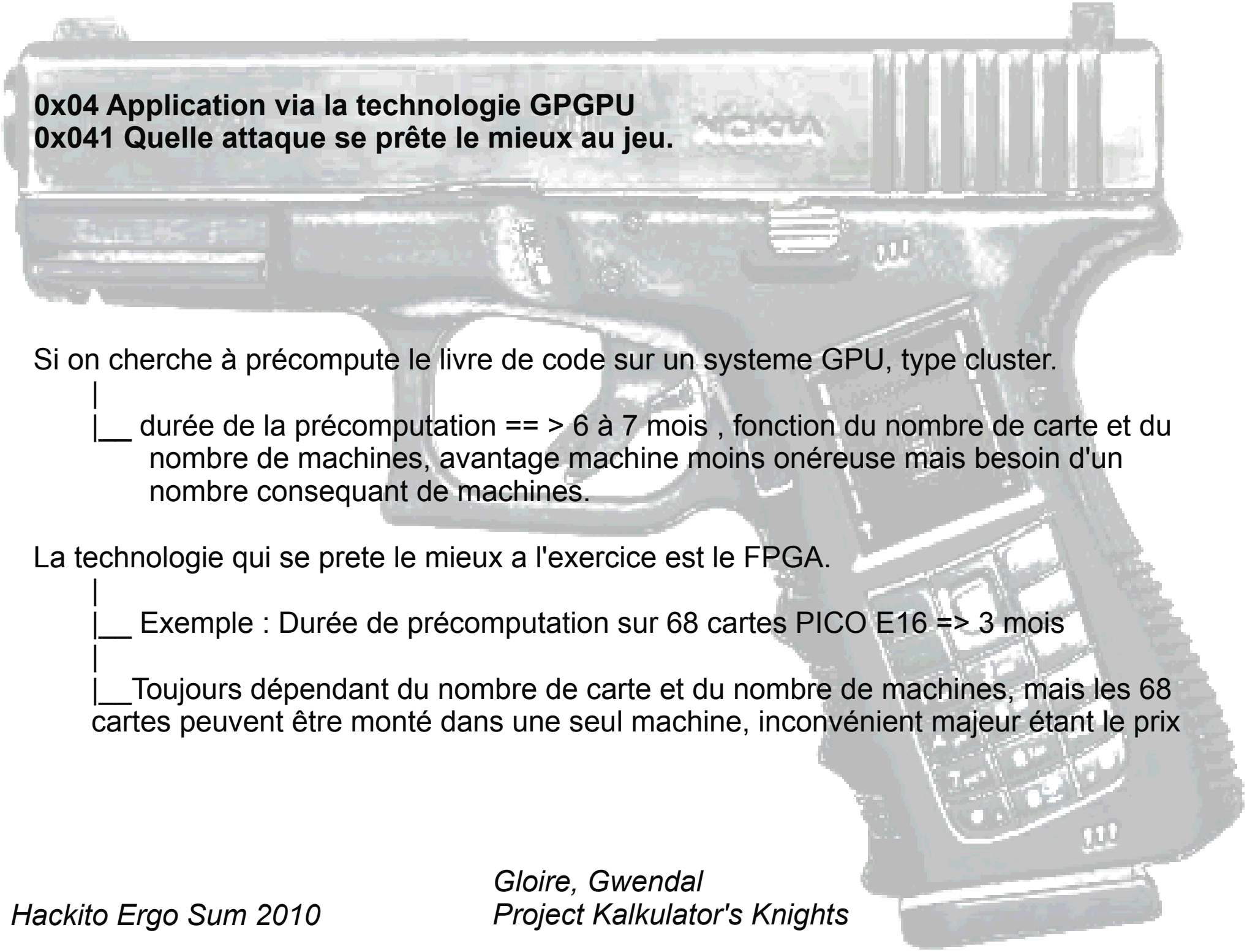
En 2004, Maximov et son équipe améliorent cette derniere avec 1 minute de calculs et quelques secondes de conversation en clair.

|
|__ documentation introuvable ==> pas d'etude possible :s

En 2009, kartsen Nohl lance son projet de précomputation de rainbow table.

|
|__ Les travaux de Nohl demontrent que le calcul complet du livre de code est impossible sur une seul machine (complexité de l'attaque 2^58) ==> 128 Petabytes et le temps de pré computation est suppérieur a 100 000 ans sur un seul pc.

Gloire, Gwendal
Project Kalkulator's Knights



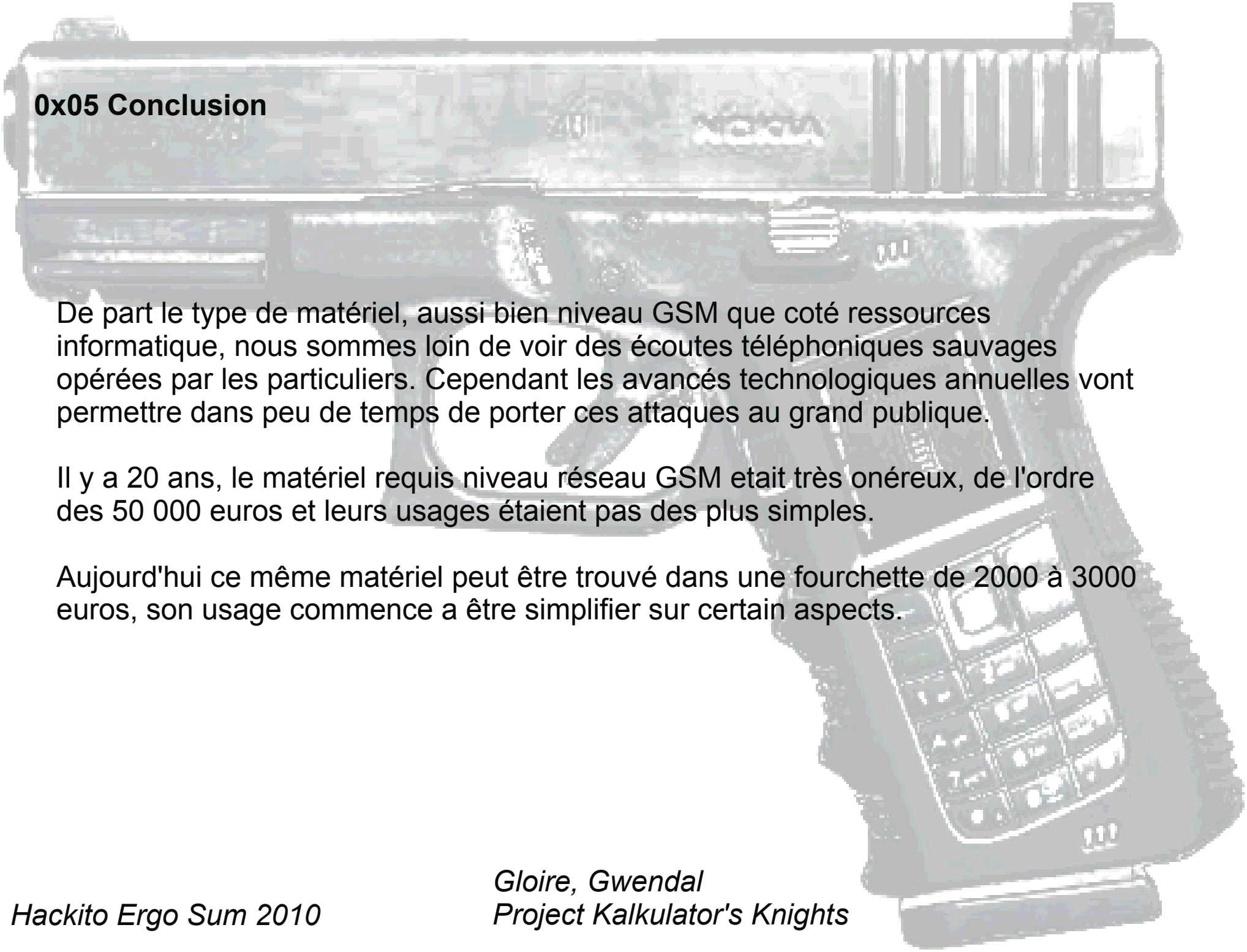
0x04 Application via la technologie GPGPU
0x041 Quelle attaque se prête le mieux au jeu.

Si on cherche à précompute le livre de code sur un systeme GPU, type cluster.

|
|__ durée de la précomputation == > 6 à 7 mois , fonction du nombre de carte et du nombre de machines, avantage machine moins onéreuse mais besoin d'un nombre consequant de machines.

La technologie qui se prete le mieux a l'exercice est le FPGA.

|
|__ Exemple : Durée de précomputation sur 68 cartes PICO E16 => 3 mois
|
|__Toujours dépendant du nombre de carte et du nombre de machines, mais les 68 cartes peuvent être monté dans une seul machine, inconvénient majeur étant le prix



0x05 Conclusion

De part le type de matériel, aussi bien niveau GSM que coté ressources informatique, nous sommes loin de voir des écoutes téléphoniques sauvages opérées par les particuliers. Cependant les avancés technologiques annuelles vont permettre dans peu de temps de porter ces attaques au grand publique.

Il y a 20 ans, le matériel requis niveau réseau GSM etait très onéreux, de l'ordre des 50 000 euros et leurs usages étaient pas des plus simples.

Aujourd'hui ce même matériel peut être trouvé dans une fourchette de 2000 à 3000 euros, son usage commence a être simplifier sur certain aspects.

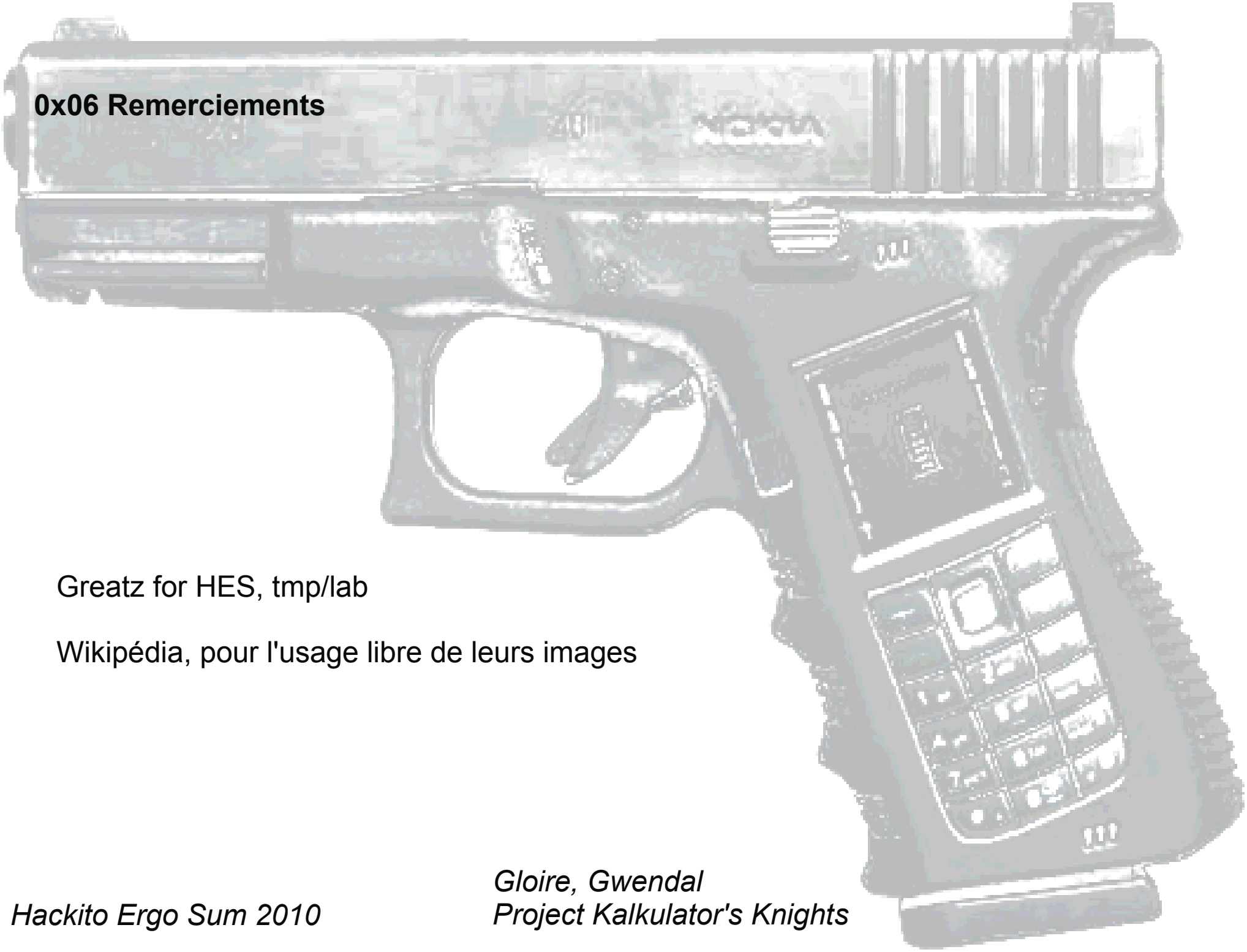
Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights

0x06 Remerciements

Greatz for HES, tmp/lab

Wikipédia, pour l'usage libre de leurs images



Hackito Ergo Sum 2010

Gloire, Gwendal
Project Kalkulator's Knights