

**GSM crypto system : A5 family
Cracking via GPU**



Hackito Ergo Sum 2010

*Gloire Gwendal
Kalkulator's Knights Project*

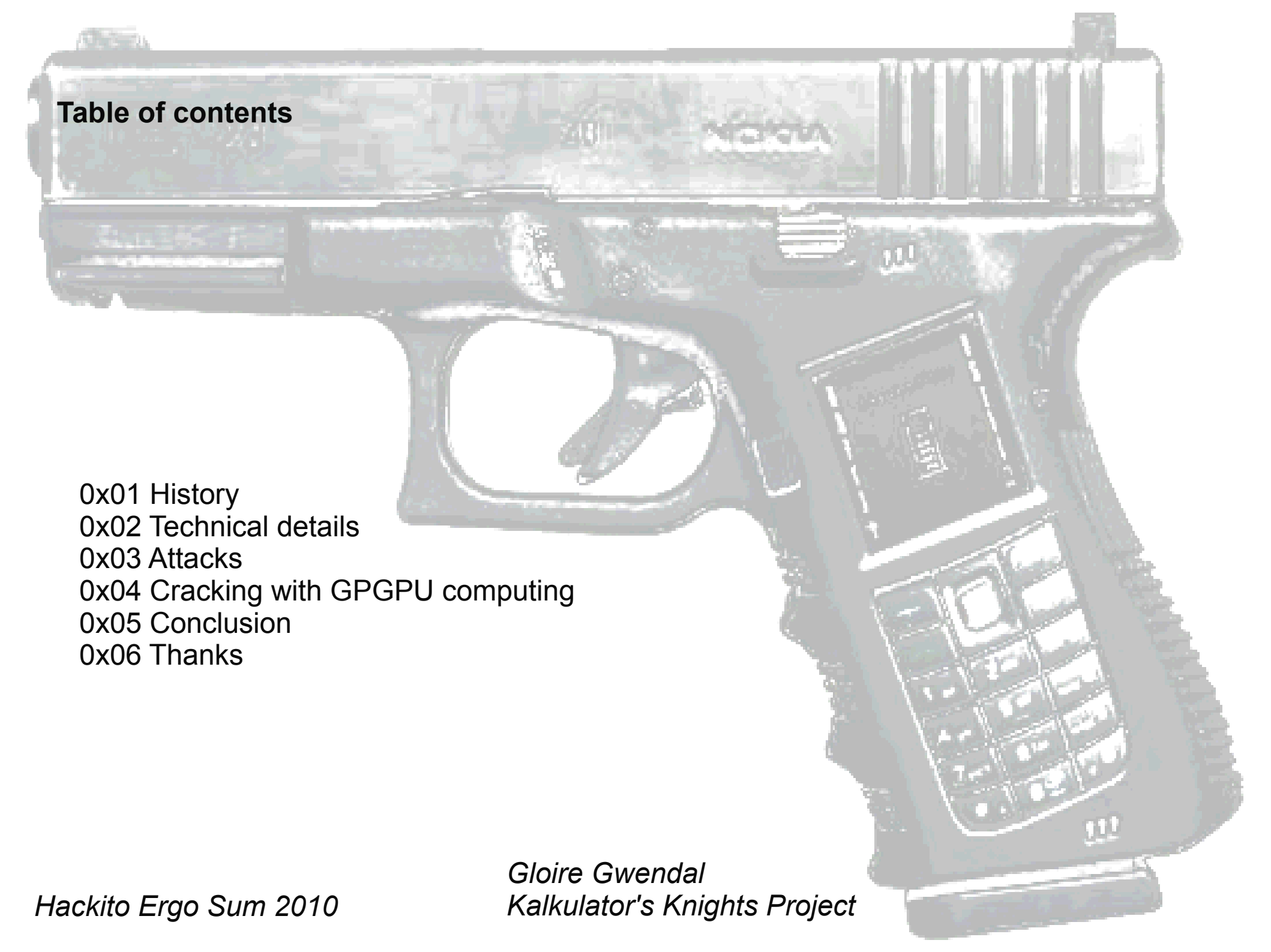
A semi-automatic handgun, possibly a Glock, is shown in a light gray, semi-transparent style. A mobile phone is attached to the grip of the handgun. The phone's screen is visible, showing a lock screen with a clock and some icons. The phone's keypad is also visible. The handgun has a slide with a textured grip and a trigger guard. The overall image has a technical or hacking theme.

Table of contents

- 0x01 History
- 0x02 Technical details
- 0x03 Attacks
- 0x04 Cracking with GPGPU computing
- 0x05 Conclusion
- 0x06 Thanks

0x01 History

- Numeric telephony begins to be used in 1982,
« GSM » group is created by « CEPT »

|
└ setting up standards

A semi-automatic handgun, likely a Glock, is shown in a light gray, semi-transparent style. A mobile phone is attached to the grip of the handgun. The phone is a candy-bar style with a small screen at the top and a full QWERTY keyboard below. The handgun's slide is partially open, and the magazine is visible. The overall image has a faded, watermark-like appearance.

0x01 History
0x011 In the 80's...

- In the 80's, numeric development in transmissions and signals handling raise
 - └ Reliable transmission methods

A semi-automatic handgun, possibly a Glock, with a mobile phone attached to the grip. The phone is a candy-bar style with a small screen and a keypad. The handgun is shown in a side profile, pointing to the right. The phone is mounted on the right side of the grip, near the trigger guard. The background is white.

0x01 History
0x012 In 1987...

- In 1987, GSM establishes technical choices:
 - └ Numeric transmissions
 - └ Temporal multiplexing of radio channels
 - └ New voice codec
 - └ Data encryption

A semi-automatic handgun, possibly a Glock, is shown in a light gray, semi-transparent style. A mobile phone is attached to the grip of the handgun. The phone is a candy-bar style with a small screen at the top and a full QWERTY keyboard below. The handgun is oriented horizontally, pointing to the left.

0x01 History
0x013 In 1991...

- In 1991, the first experimental communications are established by GSM.
- Standards are updated to ensure compatibility with new 1800Mhz networks.
- « GSM » acronym meaning changes:
 - └ « Global System for Mobile communication »

A semi-automatic handgun, possibly a Glock, is shown in a light gray, semi-transparent style. A mobile phone is attached to the grip of the handgun. The phone is a candy-bar style with a small screen at the top and a full QWERTY keyboard below. The handgun is oriented horizontally, pointing to the left. The background is white.

0x01 History
0x014 In 1994...

- In 1994, the first GSM network is deployed
 - |
 - └ Proximus (Belgium)
- Mobile assigned numbers amount is much larger than for wired ones
 - |
 - └ Still growing...

0x01 History
0x015 Timeline

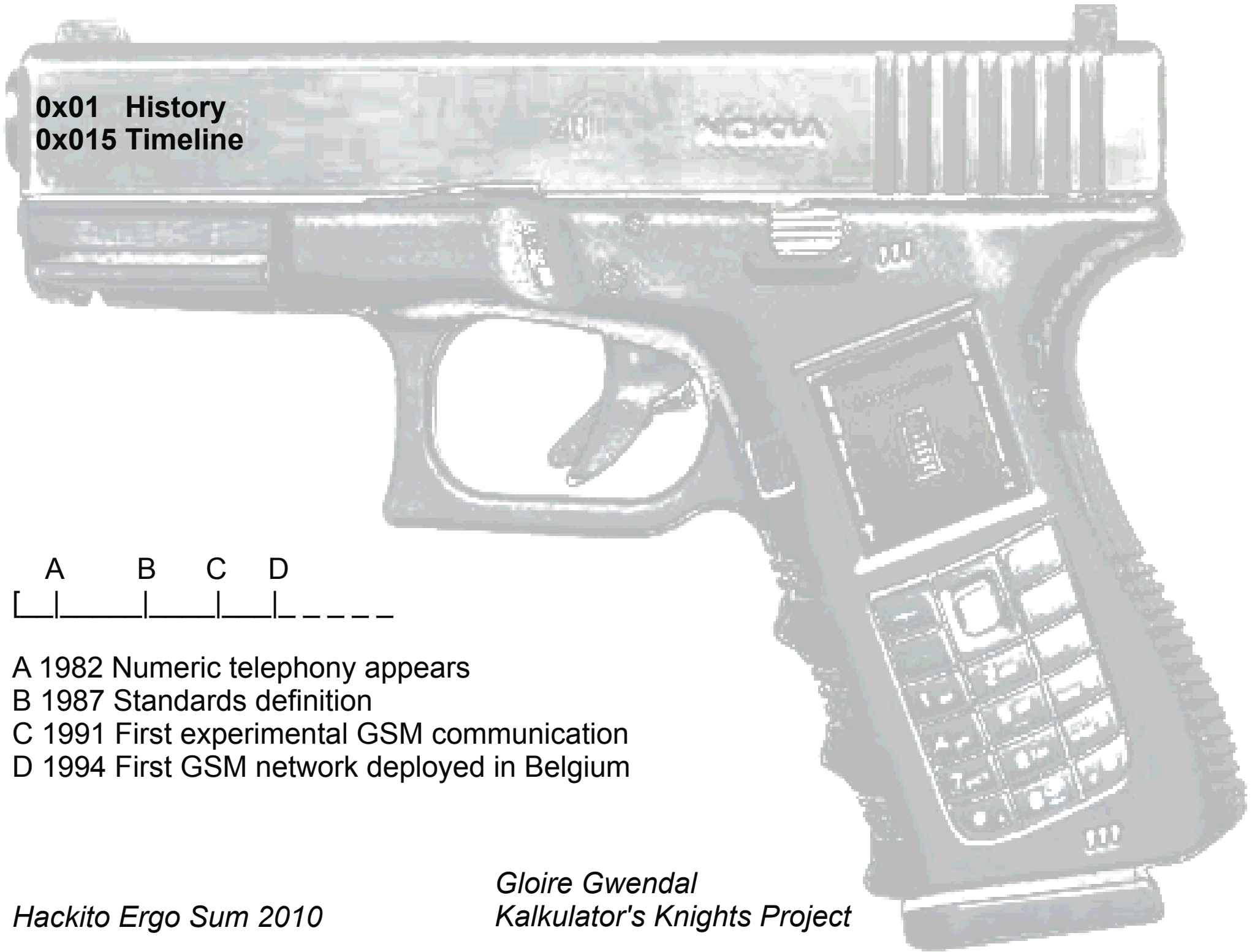


A 1982 Numeric telephony appears

B 1987 Standards definition

C 1991 First experimental GSM communication

D 1994 First GSM network deployed in Belgium



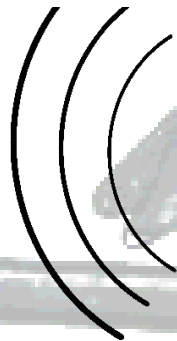
0x02 Technical details



Cellular



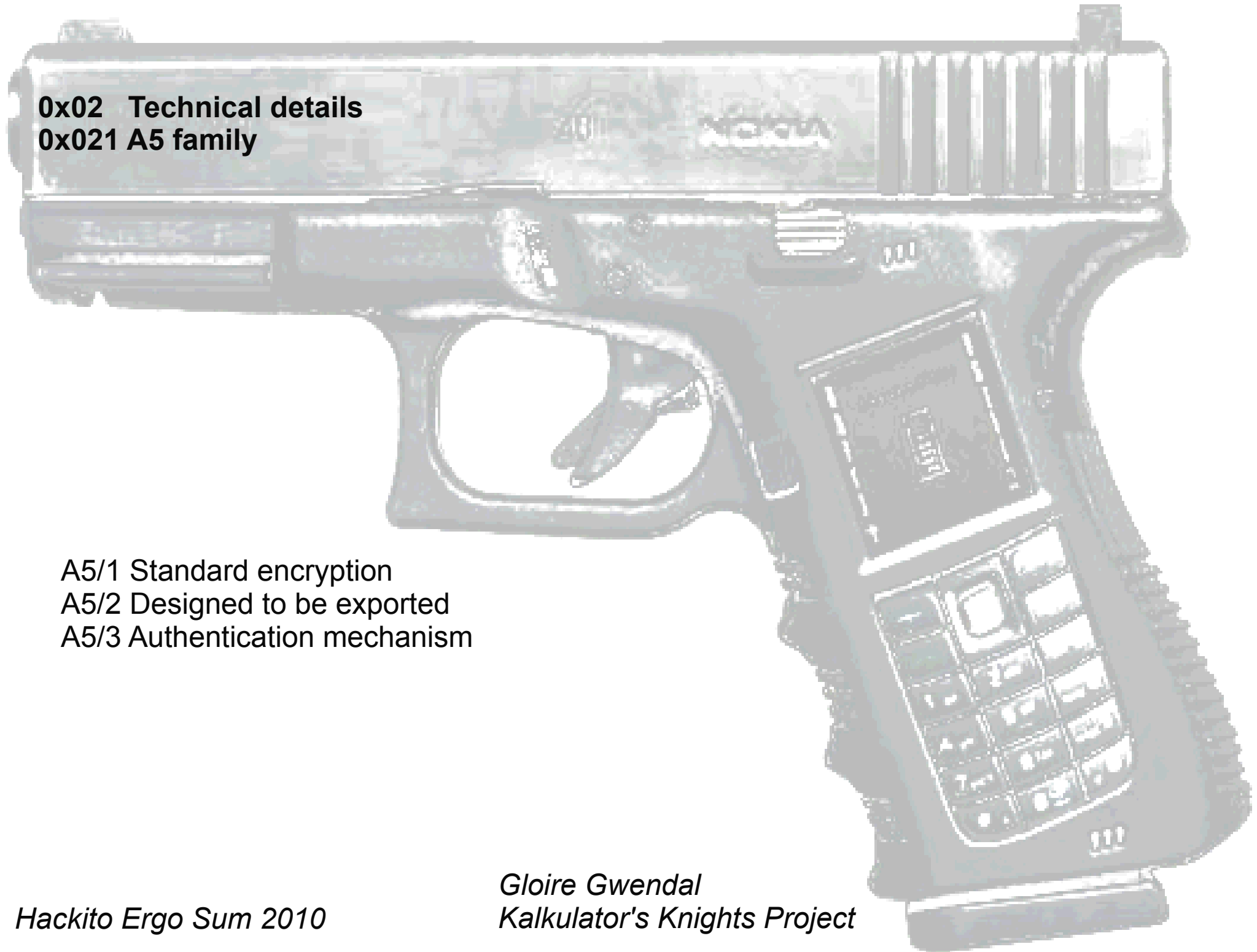
A5




Relay

0x02 Technical details
0x021 A5 family

A5/1 Standard encryption
A5/2 Designed to be exported
A5/3 Authentication mechanism

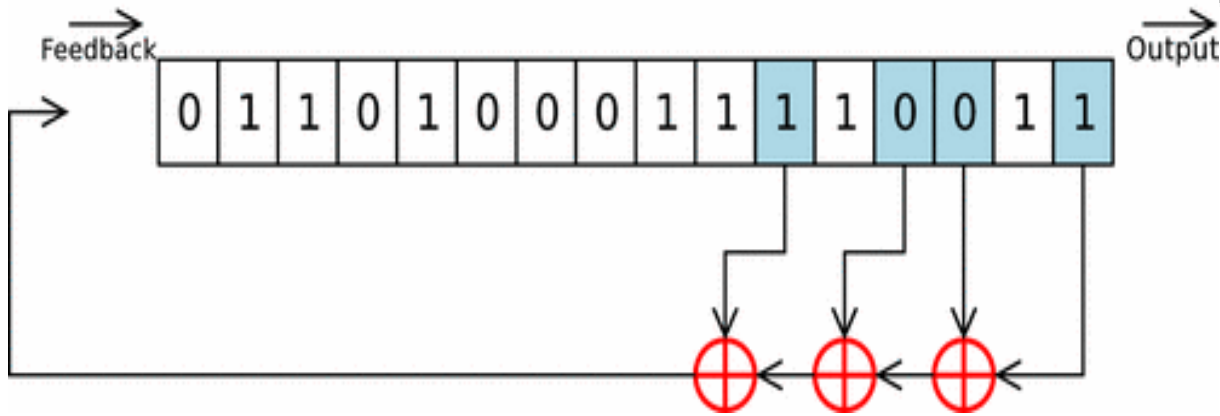




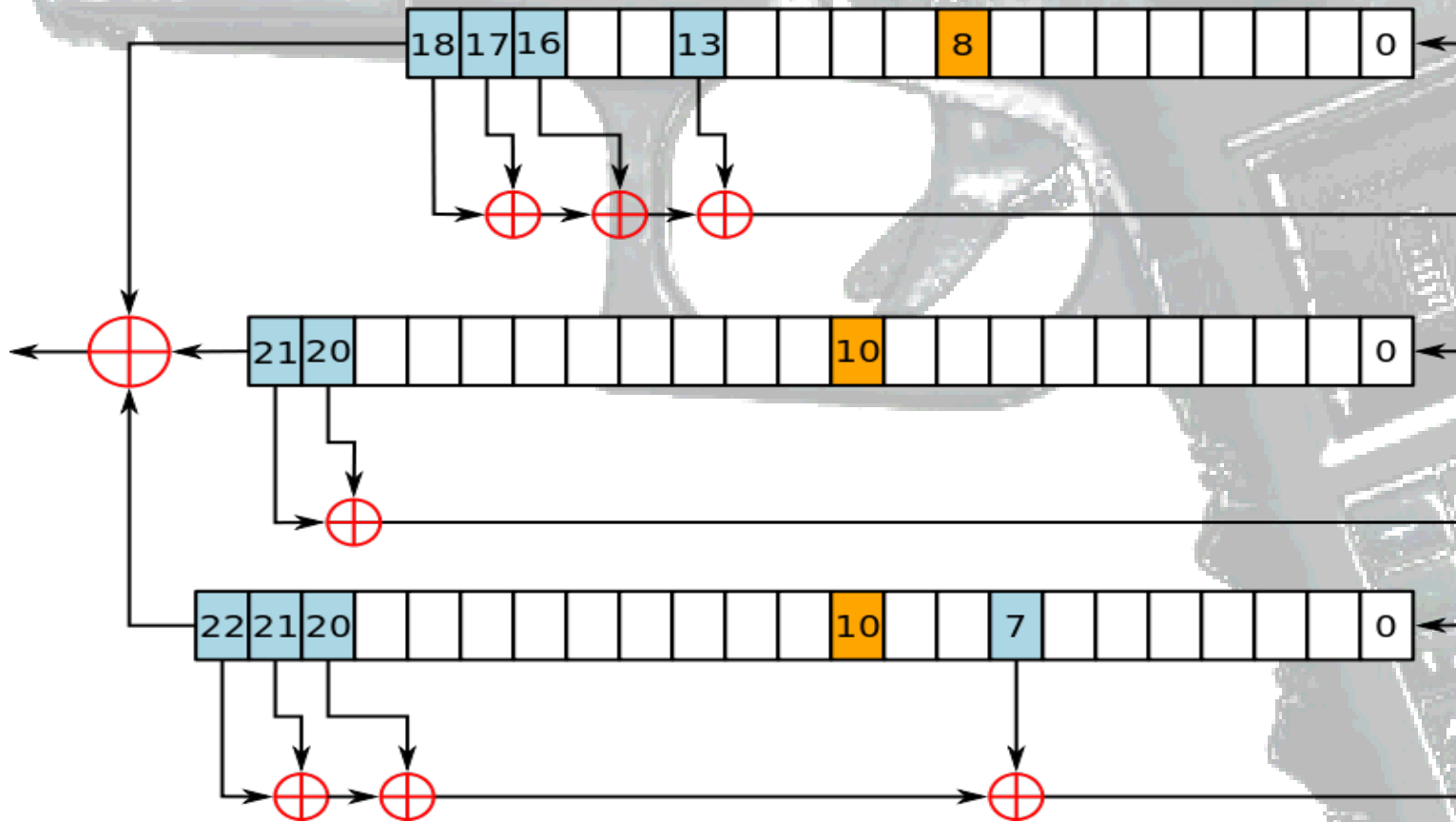
0x02 Technical details
0x022 A5/1 specifications

- Stream cipher
- Initialized by a 64bits key
- 3 registries with LSFR shifts

0x02 Technical details
0x023 LSFR registries (1st part)



0x02 Technical details
0x024 LSFR registries (2nd part)



A semi-transparent image of a handgun, likely a Glock, with a mobile phone attached to the grip. The phone is a candy-bar style with a screen and a keypad. The handgun is shown in profile, facing left. The phone is positioned vertically on the right side of the grip. The entire image is overlaid on a white background.

0x02 Technical details
0x025 Registries

T1 → Initialize the 3 registries to zero
T2 → 64 cycles while which K key is inserted
T3 → Registries shift

0x03 Attacks (1st part)

First attack made by Golic in 1997

- Linear equations system : complexity $\rightarrow 2^{40.16}$

1999, M.Briceno attacks A5/1 using reverse engineering and publishes his source code.

2000, Alex Biryukov, Adi Shamir and David Wagner make a demonstration about A5/1 real-time cryptanalysis

- Memory/time compromise, complexity $\rightarrow 2^{48}$ (with 300G of precomputed data)

The same year, Eli Biham and Orr Dunkelman publish an attack with a complexity of $2^{39.91}$ requiring to have $2^{20.8}$ bits of unencrypted data, 32Gio of data must be precomputed.

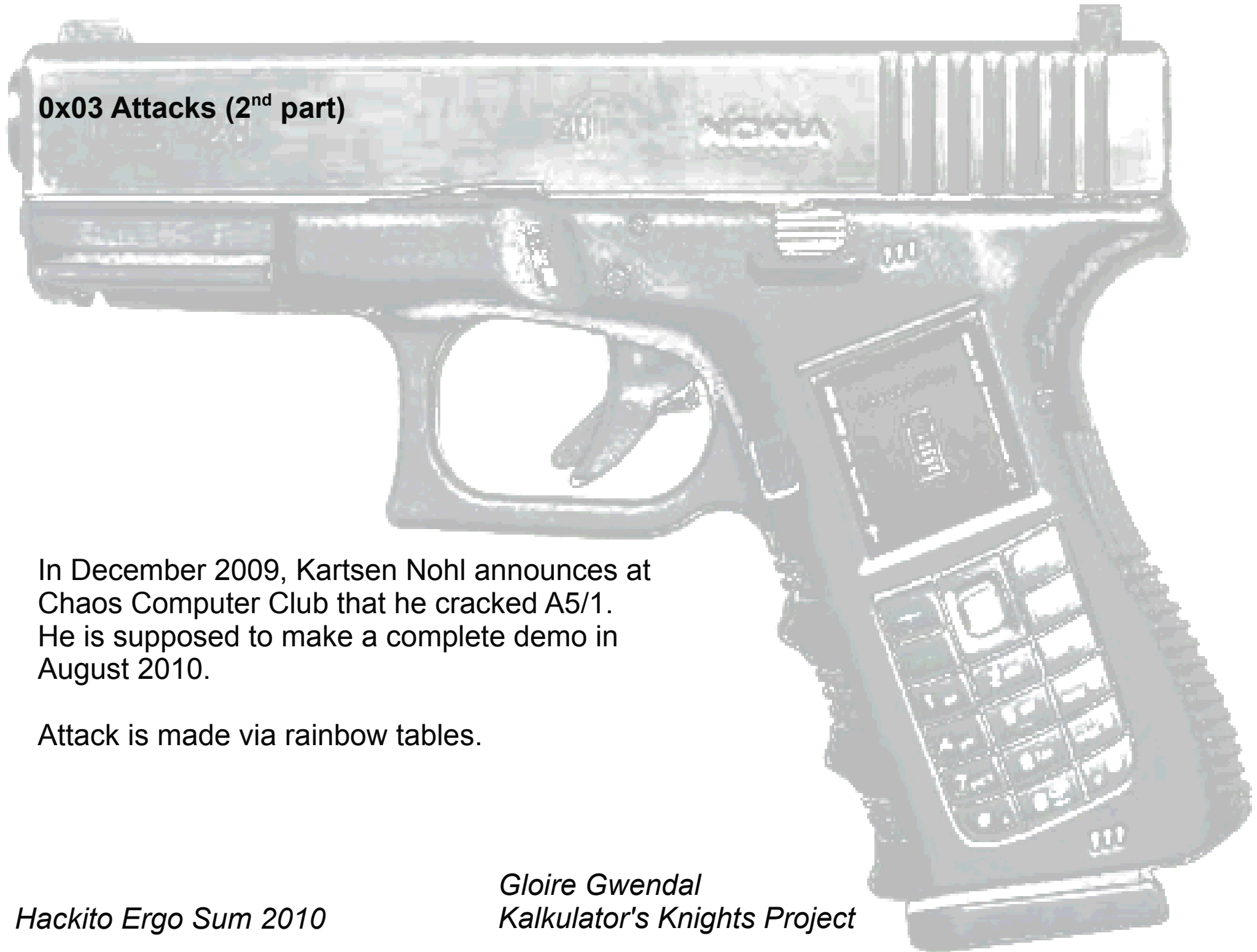
2003, Ekdahl and Johansson find an attack on A5/1 initialization, allowing the crack in a few seconds. The condition is to have 5min of unencrypted communication.

2004, Maximov and its team improve the attack with 1min of precomputing and a few seconds of unencrypted data.

0x03 Attacks (2nd part)

In December 2009, Kartsen Nohl announces at Chaos Computer Club that he cracked A5/1. He is supposed to make a complete demo in August 2010.

Attack is made via rainbow tables.



0x04 Cracking with GPGPU computing

A5/1 is a strong algorithm
|
└─ needs a lot of computing





0x04 Cracking with GPGPU computing
0x041 Which attacks are the best?

1997, Gollic publishes an attack on the key, complexity: $2^{40.16}$

— about 1 254 282 970 142 operations

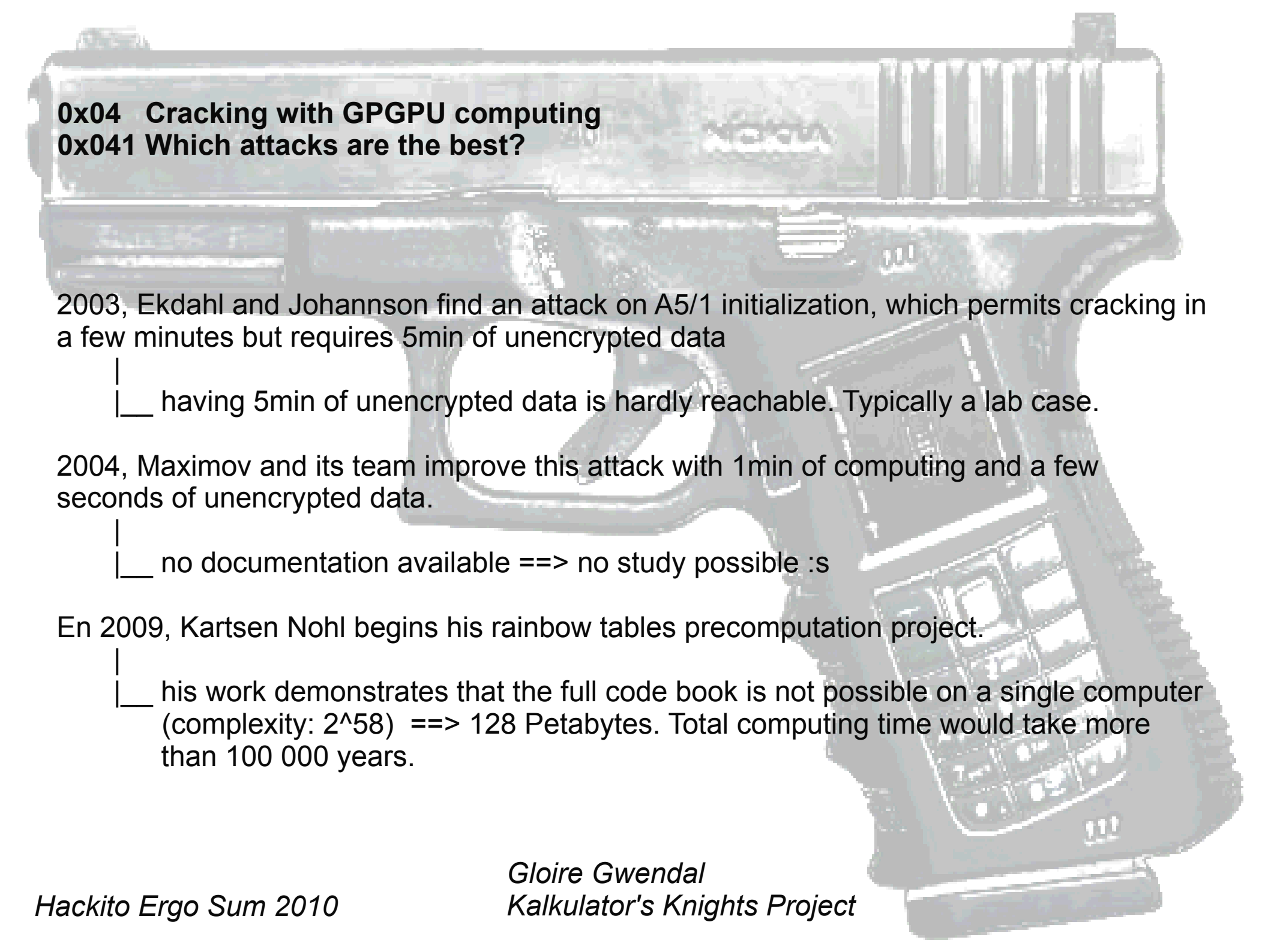
2000, Alex Biryukov, Adi Shamir and David Wagner demonstrate a real-time cryptanalysis of 15/1, complexit: 2^{48}

— 562 949 953 421 312 operations

— needs 300Go of precomputed datas

Still 2000, Eli Biham and Orr Dunkelman publish an attack with a $2^{39.91}$ complexity requiring $2^{20.8}$ bits of unencrypted data, 32 Go of data must be precomputed.

— 1 825 676.85 operations



0x04 Cracking with GPGPU computing

0x041 Which attacks are the best?

2003, Ekdahl and Johansson find an attack on A5/1 initialization, which permits cracking in a few minutes but requires 5min of unencrypted data

| ___ having 5min of unencrypted data is hardly reachable. Typically a lab case.

2004, Maximov and its team improve this attack with 1min of computing and a few seconds of unencrypted data.

| ___ no documentation available ==> no study possible :s

En 2009, Kartsen Nohl begins his rainbow tables precomputation project.

| ___ his work demonstrates that the full code book is not possible on a single computer (complexity: 2^{58}) ==> 128 Petabytes. Total computing time would take more than 100 000 years.



0x04 Cracking with GPGPU computing

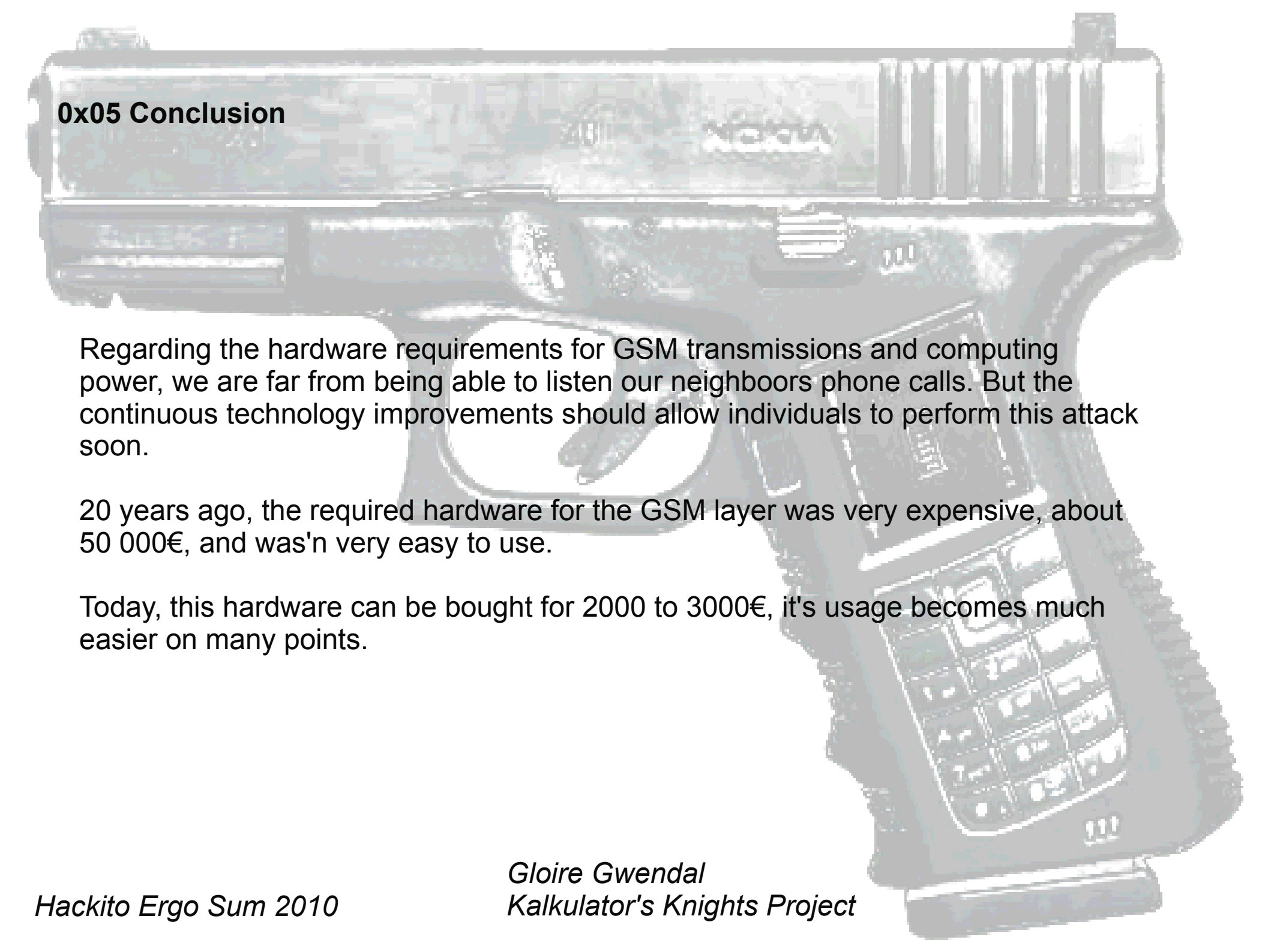
0x041 Which attacks are the best?

Precomputing the whole code book on a GPU cluster

- precomputation time == > 6 to 7 months, depending on the cards and computers amount.
Pros: cheaper
Cons: needs a lot of computers

The most appropriate technology is the FPGA:

- Example : Precomputing on 68 PICO e16 cards => 3 months
- Still depending on the processors amount, but the 68 cards can be shipped in a single machine.
Cons: expensive

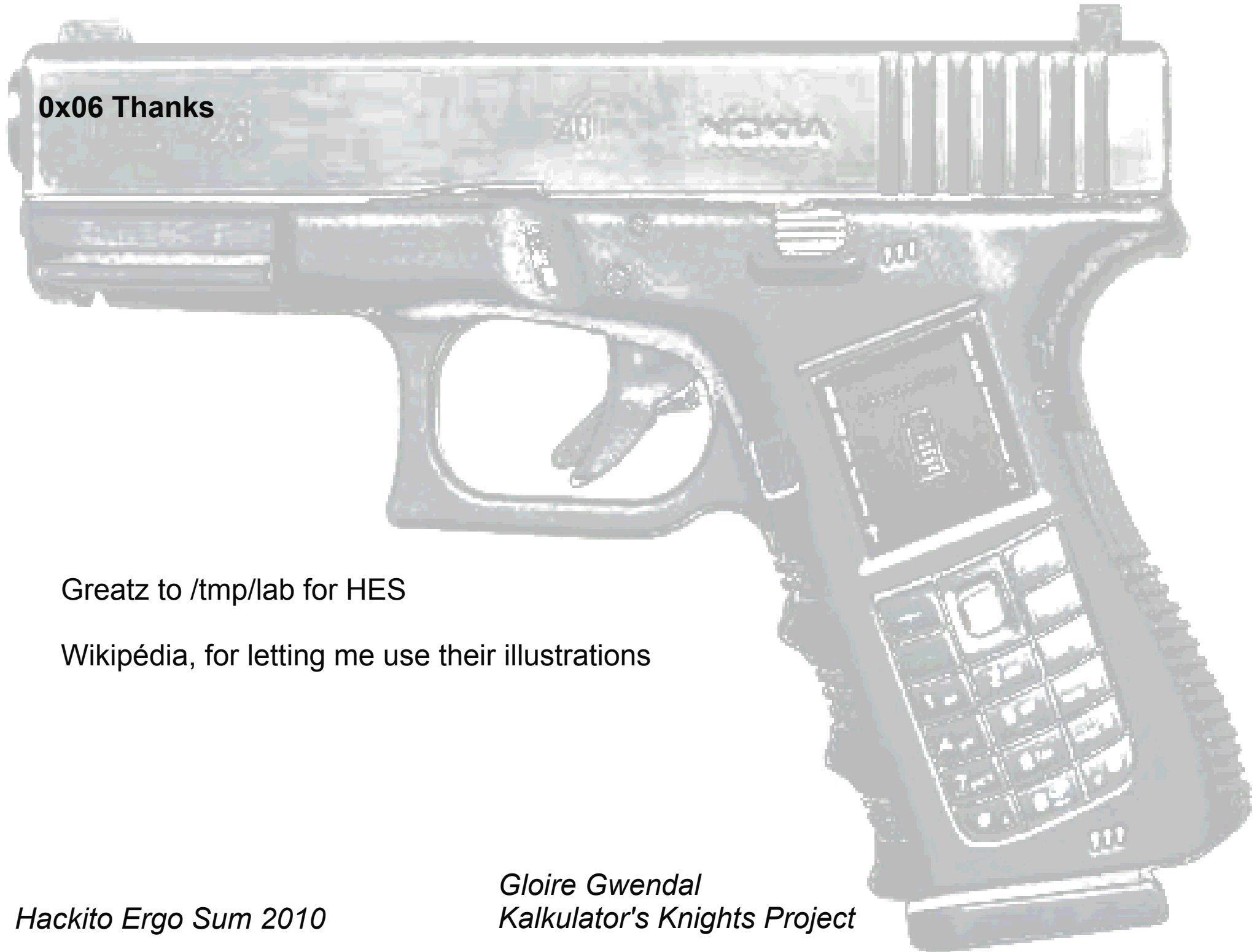


0x05 Conclusion

Regarding the hardware requirements for GSM transmissions and computing power, we are far from being able to listen our neighbors phone calls. But the continuous technology improvements should allow individuals to perform this attack soon.

20 years ago, the required hardware for the GSM layer was very expensive, about 50 000€, and wasn't very easy to use.

Today, this hardware can be bought for 2000 to 3000€, it's usage becomes much easier on many points.



0x06 Thanks

Greatz to /tmp/lab for HES

Wikipédia, for letting me use their illustrations

Hackito Ergo Sum 2010

*Gloire Gwendal
Kalkulator's Knights Project*