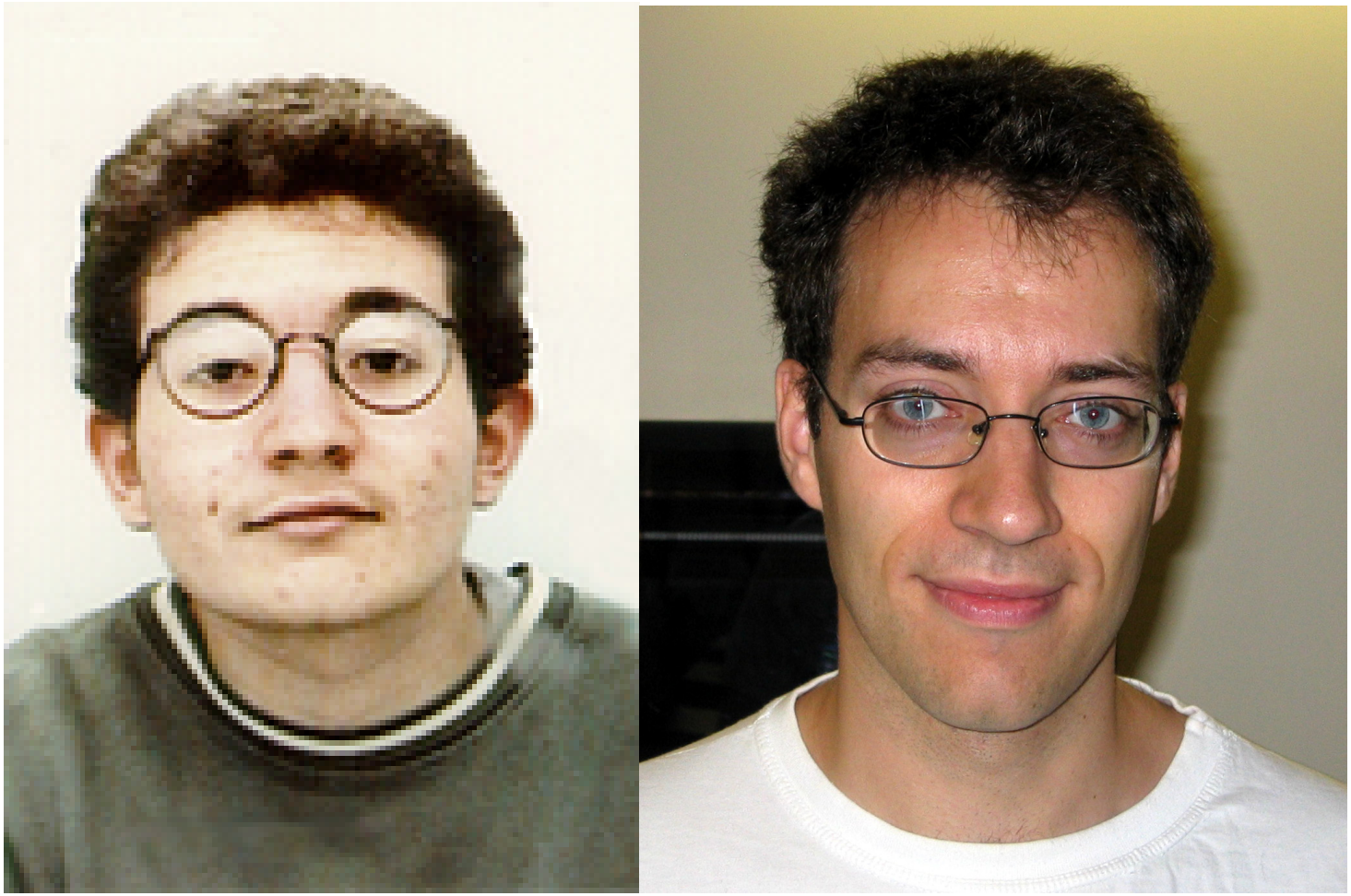
An Exercise in Shooting Yourself in the Foot: Automating the Cryptographer

Gilles Barthe[2] *Edvard Fagerholm*[1] Dario Fiore[2]
Andre Scedrov[1] Benedikt Schmidt[2]

[1]University of Pennsylvania [2]IMDEA Software Institute

August 19, 2014

Cryptographers



ographers – Now Obsolete

Synthesis

Goal: Automatically discover new crypto constructions.

Synthesis

Goal: Automatically discover new crypto constructions.

Story so far

- 90s crypto (padding-based encryption, modes of operation).
- This talk: structure-preserving signatures (CRYPTO 2014).
- Based on generic group analyzer tool.

Overview of Synthesis Steps

Steps to synthesize structure-preserving signatures:

1. Choose random formulas for signature (from template).
2. Log if potential scheme, i.e. there is a verification equation.
3. Check potential schemes for security.

Can often directly jump to 3rd step if we have a clear goal that we are looking for.

Automatic Generation of a CRYPTO 2014 Paper

Example

Type II bilinear group $e : G_1 \times G_2 \to G_T$, generators g_1, g_2, g_t.
Assume keys of form:

$$\text{Private: } v, w \in \mathbb{Z}_p \quad \text{Public: } V = g_1^v, \ W = g_1^w$$

Signatures a pair $(R, S) \in G_2^2$, where

$$\begin{aligned} R &= g_2^r, & r &\xleftarrow{\$} \mathbb{Z}_p, \\ S &= M^{P(v,w,r)} g_2^{Q(v,w,r)}, & P, Q &\in \mathbb{Z}[X, X^{-1}, Y, Y^{-1}, Z, Z^{-1}] \end{aligned}$$

Coeffs of P, Q in set $-1, 0, 1 \Rightarrow$ approx 1 million candidates for P, Q.

Automatic Generation of a CRYPTO 2014 Paper

May brute-force all candidates in a few minutes. Finds e.g. following scheme:

$$\begin{aligned} \textbf{Signature:} \quad & R = g_2^r, \quad S = M^{w/r} g_2^{v/r} \\ \textbf{Verification:} \quad & e(\psi(R), S) = e(V, g_2) e(W, M) \end{aligned}$$

Scheme has the following properties:

- Existentially unforgeable under adaptive chosen message attack.
- Randomizable: Sample $r' \xleftarrow{\$} \mathbb{Z}_p^\times$, set $(R', S') = (R^{r'}, S^{1/r'})$.
- $e(V, g_2)$ can be precomputed $\Rightarrow$ needs two pairings for verification in addition to one application of $\psi : G_2 \to G_1$.
- Compare to three pairings for similar scheme by Abe et al. at CRYPTO'14.

(Disclaimer: Abe et. al have some other stuff in the paper too...)

How Tool Works

In the previous example the tool works as follows:

1. Searches for verification equation.
2. When found create interactive problem for security analysis.

Interactive GGM problem for $R = g_2^r, \quad S = M^{w/r} g_2^{v/r}$

```
map G1 * G2 -> GT.
iso G2 -> G1.
input [V,W] in G1.
oracle o1(M:G2) =
  sample R;
  return [ R, V*R^-1 + M*W*R^-1 ] in G2.

win (wM:G2, wR:G2, wS:G2) =
  (wM <> M /\ 0 = V + W*wM - wR*wS).
```