An Authentication Scheme based on Roots of Sparse Polynomials

Amin Shokrollahi
EPFL

Joint work with J. von zur Gathen and I. Shparlinski

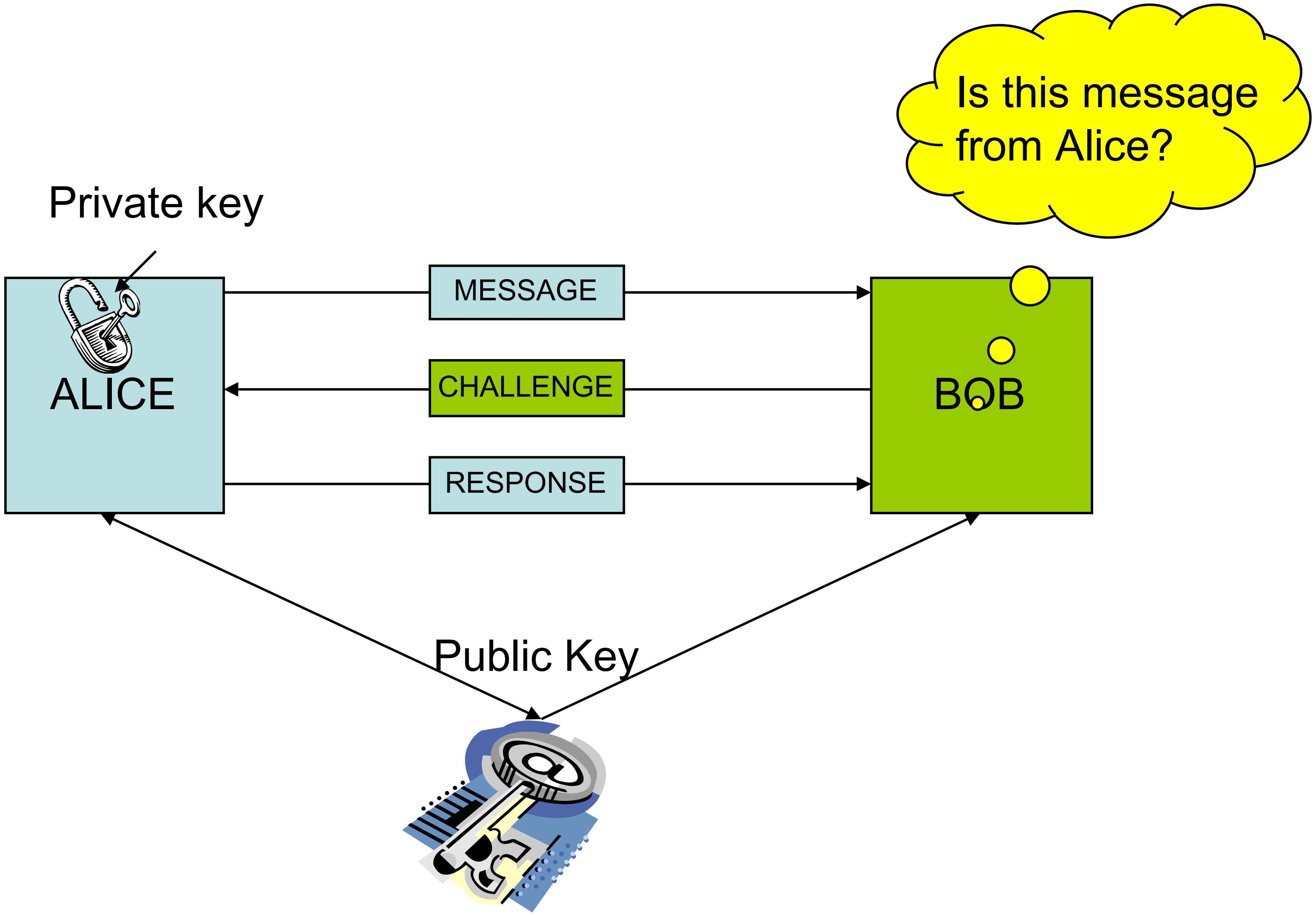
What We Will Do

- Introduce a new authentication and signature scheme based on roots of sparse polynomials
- Show that original scheme is not secure
- Give a revised scheme that does not have the clear disadvantages of the original scheme

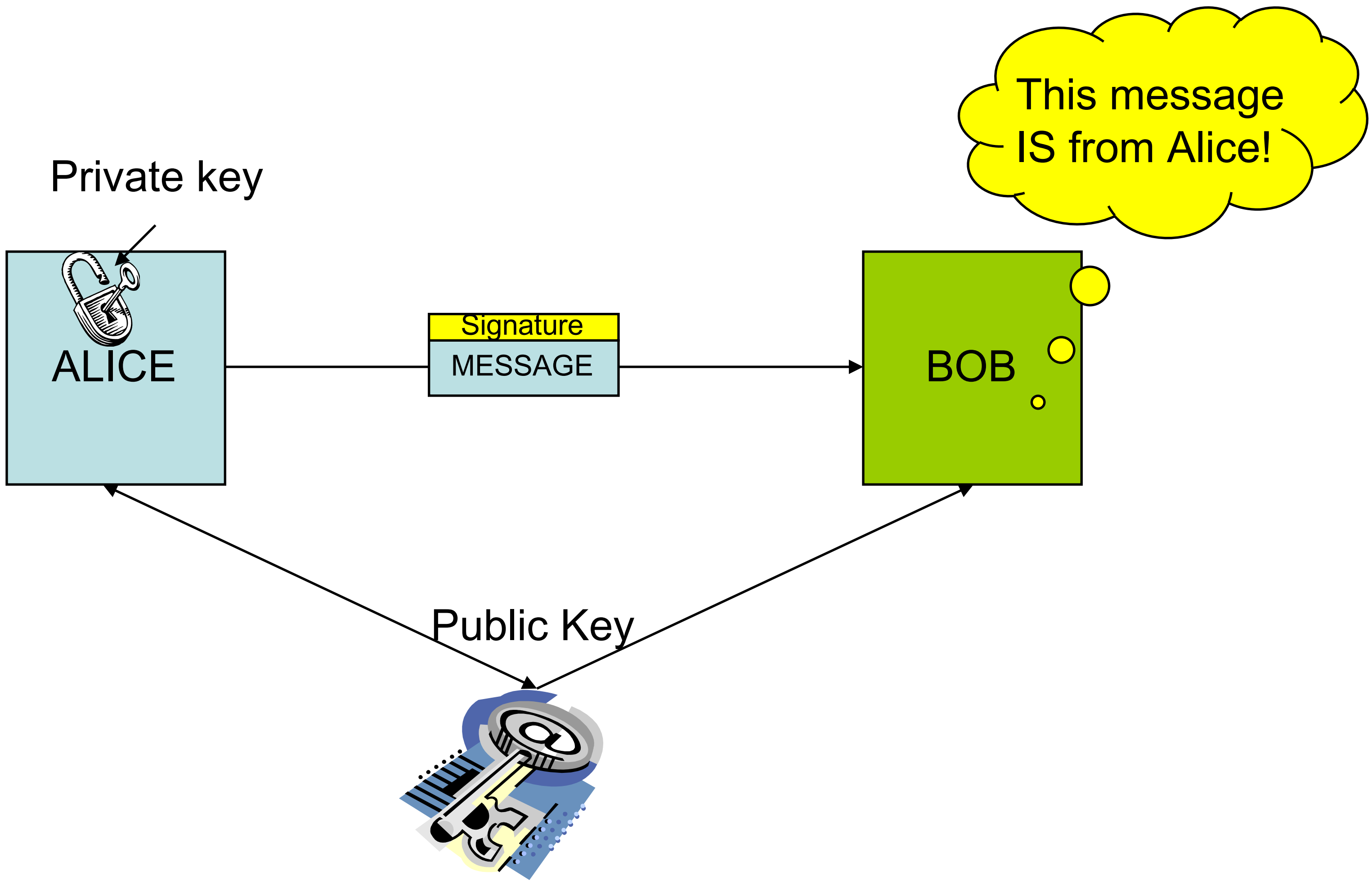
What We Will Not Do

- Give a detailed cryptoanalysis of our scheme
- Specify parameters for which the scheme could be used
- Discuss practical applications

Message Authentication



Signature Schemes



Some Known Public Key Schemes

- RSA based schemes
  - SSH
- Discrete log based schemes
  - DSA
- Elliptic curve based schemes
  - ECDSA

Security is based on hardness of factoring, or hardness of discrete logs.

Our Scheme – Part I

Use sparse system of equations in variables $X_1, X_2, \ldots, X_n$ which has many integer roots $(a_{11},\ldots,a_{1n}), \ldots, (a_{m1},\ldots,a_{mn})$.

Publish the system of equations (public key).

Challenge by Bob is a prime number p.

Response is a solution of the system modulo p.

Is based on hardness of solving systems of equations modulo primes.

Private Key

Representation of the system that facilitates finding the roots!

Example: Want roots (0,3) and (2,-3).

Find a, b, c, d such that

$$a\,x^3y + b\,xy^2 - x^4 + xy - 6 = 0$$
$$c\,xy^4 + d\,x^5 + x^3y^2 + 5x^4y^3 - 13xy + 3 = 0$$

for (x,y) in { (0,3), (2,-3)}.

Four equations in four unknowns.

In General

- Choose the roots
- Choose the exponents and part of the equations (sparsity!)
- Solve for the other part of the equations using Gaussian elimination (for example), or lattice reduction.

Is the Scheme Secure?

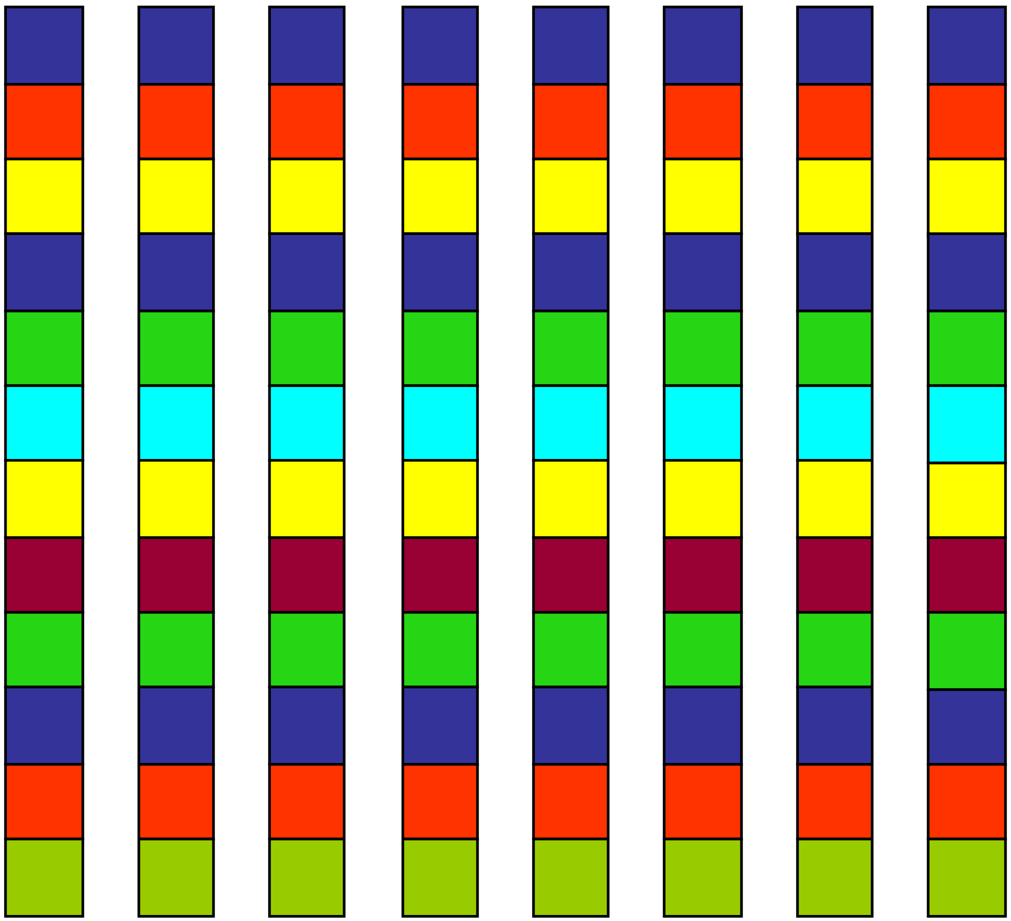
- Attacker can challenge Alice many times, each time receiving some $(a_{i1},\ldots,a_{in}) \bmod p_i$.

- Attacker wants to collect enough information to recover some root of the system. Then attacker can impersonate Alice.

Is the System Secure?

- If Alice uses only one root, then attacker can use Chinese remaindering techniques to calculate the root.
- Alice has to change the roots often.
- After N challenges attacker has gathered n vectors of length N for each of the coordinates.
- Within each such vector N/m values correspond to the same root.

Is the Scheme Secure?



$(a_{91},\ldots,a_{9n}) \bmod p_1$

$(a_{41},\ldots,a_{4n}) \bmod p_2$

$(a_{71},\ldots,a_{7n}) \bmod p_3$

$(a_{91},\ldots,a_{9n}) \bmod p_4$

$(a_{21},\ldots,a_{2n}) \bmod p_5$

$(a_{81},\ldots,a_{8n}) \bmod p_6$

$(a_{71},\ldots,a_{7n}) \bmod p_7$

$(a_{31},\ldots,a_{3n}) \bmod p_8$

$(a_{21},\ldots,a_{2n}) \bmod p_9$

$(a_{91},\ldots,a_{9n}) \bmod p_{10}$

$(a_{41},\ldots,a_{4n}) \bmod p_{11}$

$(a_{01},\ldots,a_{0n}) \bmod p_{12}$

Chinese Remaindering with Errors

Fix a hypothetical root.

Each vector has at least N/m correct values, and N-N/m incorrect ones.

Use list-decoding of Chinese Remainder Codes (Goldreich et al., Boneh, Guruswami et al.) to correct the errors and find the correct values.

For large N these algorithms succeed provided that N is at least cm^2, where c is small compared to m.

So, scheme is NOT secure!

Our Scheme – Part II

- Choose the roots in a hidden number field K.
- Create the equations over the integers.
- Allow only challenge primes that are completely split in K.
- For each challenge prime p take some prime ideal $\mathfrak{p}$ of degree one dividing p in K, and output $(a_{i1},\ldots,a_{in})$ mod $\mathfrak{p}$.

Does the Hidden Number Field Help?

Shparlinski and Steinfeld have devised an algorithm which can calculate the minimal polynomial of the element a from the vector

(a mod p_1, a mod p_2, …., a mod p_N).

Such an algorithm would break the scheme if we could efficiently identify which of the responses correspond to the same root of the system of equations.

A modification of list-decoding could provide such a method. So, Approach II may not be secure.

Our Scheme – Part III

- Use a hidden rational surface to obtain infinitely many solutions.

- Obscure the rational surface using random linear transformations.

Approach has the problem that the bit-complexity of the authentication increases (mildly) with number of challenges, since roots with ever larger coefficients need be used to avoid list-decoding attack.

Conclusion

- Authentication schemes based on sparse polynomials provide interesting alternatives to RSA, discrete-log, or Elliptic Curve methods.
- Several flavors of one such method was presented in this talk, and some of the flavors were proved insecure using list-decoding of Chinese Remainder Codes.
- Other flavors need more rigorous study to prove (or disprove) themselves.