Cryptography in an Unbounded Computational Model

David P. Woodruff

MIT Laboratory for Computer Science,
Cambridge, USA

joint work with Marten van Dijk
(Philips Research, MIT-LCS)

Contents:

1. Unbounded computational model

All parties compute as follows:

- Start with two numbers $\{0, 1\}$
- Work with the field operations $\{+, -, *, /\}$
- Have unbounded computational time

Parties can generate the rational numbers $\mathbb{Q}$.

Enumeration Attack:

For each rational q,

- Run public verification algorithm on q to determine if q is the shared secret.

1. Unbounded computational model

Prevent enumeration attacks with extensions to model:

- Can sample any finite number of real numbers from the interval [0,1].

- Can store any irrational number in a single, infinite-precision register.

Parties can generate fields of the form

$$\mathbb{Q}(r_1, \ldots, r_n)$$

- $\{r_i\}$ arbitrary real numbers

1. Unbounded Computational Model Now do enumeration attacks succeed? *No.* Fields generated are still countable,

2. An identification protocol

Alice first samples a random real number r, and publishes its square $r^2 = p$. r is her secret key, p is her public key.

1. Alice samples a real number s. She gives Bob $t = s^2$.

2. Bob flips a coin and tells Alice the result.

3.
   - If Bob said "heads", then Alice gives Bob s, and Bob checks that $s^2 = t$.
   - If Bob said "tails", then Alice gives Bob $u = rs$, and Bob checks that $u^2 = pt$.

The above protocol is based on the impossibility of computing the exact square root of an

3.a. The impossibility of secure public-key encryption schemes

$$\begin{array}{ccccc} \text{Public} & & \text{Encrypter} & & \text{Decrypter} \\ \mathbb{Q}(PK,c) & \subseteq & \mathbb{Q}(PK,m) & \subseteq & \mathbb{Q}(SK,c) \end{array}$$

(PK,SK): (public key, secret key)-pair
(m,c): (message, ciphertext)-pair using SK

Proof:

1. $\mathbb{Q}(SK,c) = \mathbb{Q}(SK,m)$

2. $[\mathbb{Q}(SK,c) : \mathbb{Q}(PK,c)] = [\mathbb{Q}(SK,m) : \mathbb{Q}(PK,m)]$

3. $\mathbb{Q}(PK,m) = \mathbb{Q}(PK,c)$

3.b. The impossibility of secure signature schemes

Pub. Before Sig		Pub. After Sig		Signer
$\mathbb{Q}(PK, m)$	$\subseteq$	$\mathbb{Q}(PK, m, s)$	$\subseteq$	$\mathbb{Q}(SK, m)$

(s, m): (signature, message)-pair using SK

Proof:

1. Bijection $f : L \to L(m)$ of intermediate fields $\mathbb{Q}(PK) \subseteq L \subseteq \mathbb{Q}(SK)$ to intermediate fields $\mathbb{Q}(PK, m) \subseteq L(m) \subseteq \mathbb{Q}(SK, m)$

2. After m is signed, public learns L' where $\mathbb{Q}(PK) \subset L' \subset \mathbb{Q}(SK)$, where the inclusions are proper inclusions.

3. Hence, nonzero probability there exists a

3.c.i. The impossibility of establishing a shared secret

The impossibility of establishing a shared secret will immediately rule out public-key encryption, interactive encryption, Diffie-Hellman key exchange, and oblivious transfer in this model.

A protocol between Alice and Bob consists of a sequence of steps. Let F_A be the field generated by Alice and let F_B be the field generated by Bob. During each step information may be revealed to the public. Let F_P be the field generated by the public information.

There are two types of steps, either Alice (Bob) selects a random element thereby extending her associated field or Alice (Bob) transmits an element from her field to Bob (Alice). Due

3.c.ii. The impossibility of establishing a shared secret

We have the two basic steps for Alice (and similarly for Bob):

Step 1 *A transcendental element x over $\mathbb{Q}(F_A, F_B)$ is selected by Alice:*

$$(F_A, F_B, F_P) \to (F_A(x), F_B, F_P),$$

Step 2 *Alice selects an element x in F_A and transmits it to Bob:*

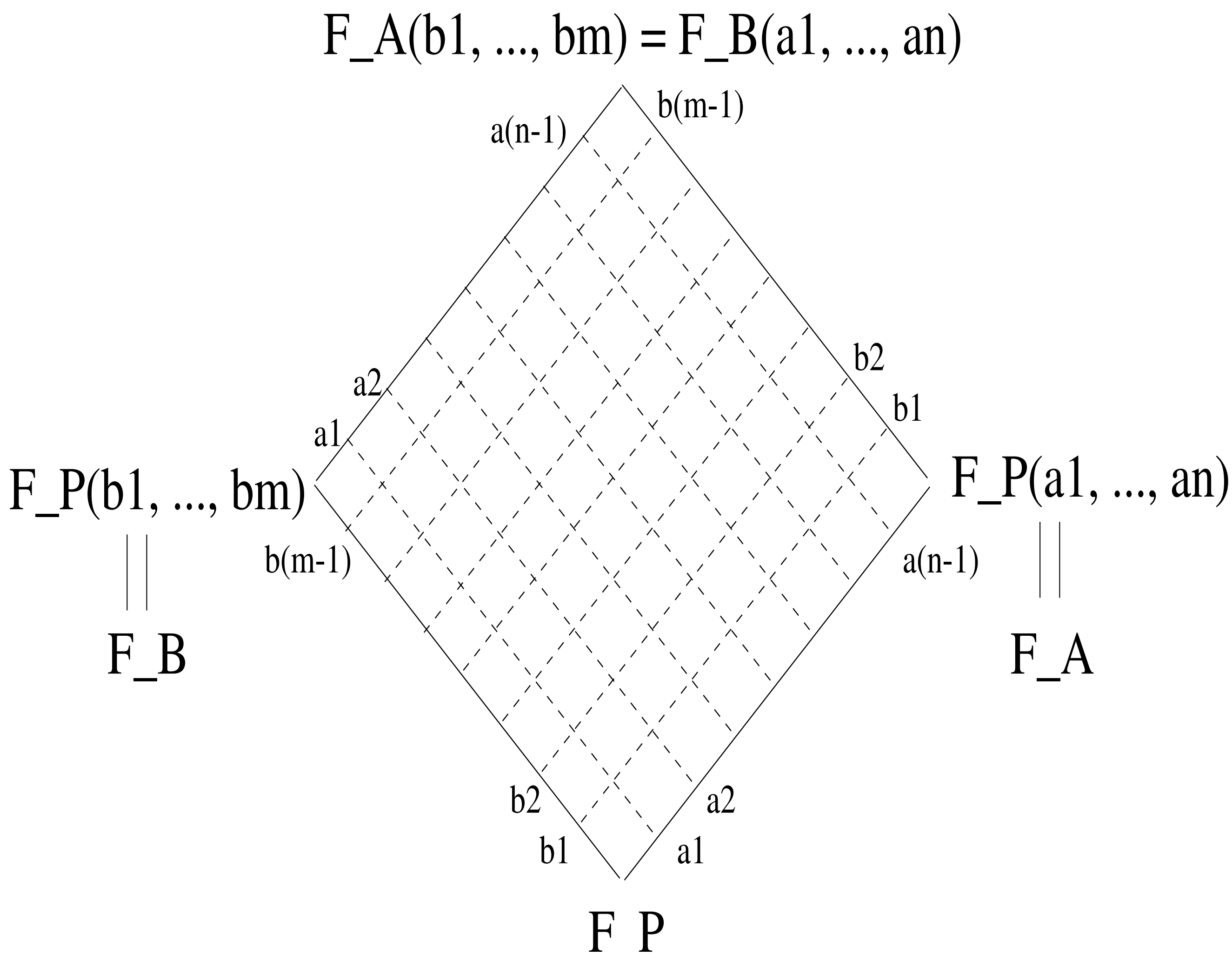
$$(F_A, F_B, F_P) \to (F_A, F_B(x), F_P(x)),$$

To show the impossibility of secret sharing over rational numbers we need to prove

$$F_A \cap F_B = F_P$$

after each step of the protocol. In other words

3.c.iii. The impossibility of establishing a shared secret



Invariant: $\forall i, 0 \leq i \leq n-1,$

3.c.iv. The impossibility of establishing a shared secret

Lemma 1: Let $G \subseteq F$ be fields such that $[G(v) : G] = [F(v) : F]$. Then either v is transcendental over F or there exists a basis $\mathcal{X} = \{1, v, v^2, \ldots, v^{n-1}\}$ of $F(v)$ over F which is also a basis of $G(v)$ over G.

Proof: The basis $\mathcal{X}$ of $F(v)$ over F is linearly independent over $G \subseteq F$. Since $[G(v) : G] = [F(v) : F]$ and $\mathcal{X}$ does not depend on F, $\mathcal{X}$ is a basis of $G(v)$ over G.

Lemma 2: Let $G \subseteq F$ and let v be tranceden-tal over F. Then $F \cap G(v) = G$.

Proof: Let $x \in G(v)$. Then there exist polyno-mials $f(.)$ and $g(.)$ with coefficients in $G \subseteq F$ and $g(v) \neq 0$ such that $x = f(v)/g(v)$. If x is

3.c.v. The impossibility of establishing a shared secret

One can generalize the previous lemma to:
Lemma 3: Let $G \subseteq F$ and let $\mathcal{X}$ be a finite linear independent set over F with $1 \in \mathcal{X}$. Then $F \cap G[\mathcal{X}] = G$. (We omit the proof)

Finally, the result we shall need:
Lemma 4: The invariant implies $\forall i$,

$$F_A(a_1, \ldots, a_i) \cap F_P(a_1, \ldots, a_i) \subseteq$$

$$F_A(a_1, \ldots, a_i) \cap F_P(a_1, \ldots, a_{i-1})$$

Proof:
Let $F_i = F_A(a_1, \ldots, a_i)$ and $G_i = F_P(a_1, \ldots, a_i)$. By lemma 1, the invariant implies either a_{i+1} is transcendental over F_i or there exists a basis $\mathcal{X}$ of $F_i(a_{i+1})$ over F_i which is also a basis of $G_i(a_{i+1})$ over G_i. According to lemmas 1 and 2 respectively, $F_i \cap G_i(a_{i+1}) = G_i$. Since

3.c.vi. The impossibility of establishing a shared secret

It can be shown that both steps (and hence the entire protocol) preserve the invariant. It remains to show that the invariant implies

$$F_A \cap F_B = F_P$$

Proof:

1. $F_P \subseteq F_A \cap F_B$ since F_P is public.

2. $\forall i$,

$$F_A(a_1, \ldots, a_i) \cap F_P(a_1, \ldots, a_i) \subseteq$$

$$F_A(a_1, \ldots, a_i) \cap F_P(a_1, \ldots, a_{i-1})$$

Conclusion

In summary, we have shown that although identification protocols and one-way functions exist in this model, secure signature schemes, secure encryption schemes, and schemes for sharing a secret do not.

Future work:

- Work was motivated by Burmester, Rivest, and Shamir's "Geometric Cryptography." The computational model in their paper allows the operations

  $$\{+, -, *, /, \sqrt{y} \text{ for } y > 0\}.$$

  What cryptographic primitives are possible now?

- What are necessary and sufficient condi-