DEFEATING THE BEN-ZVI, BLACKBURN, AND TSABAN ATTACK ON THE ALGEBRAIC ERASER

IRIS ANSHEL, DEREK ATKINS, DORIAN GOLDFELD, AND PAUL E. GUNNELLS

Abstract.
The *Algebraic Eraser Diffie–Hellman* (AEDH) protocol was introduced in 2005 and published in 2006 by I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux as a protocol suitable for use on platforms with constrained computational resources, such as FPGAs, ASICs, and wireless sensors. It is a group-theoretic cryptographic protocol that allows two users to construct a shared secret via a Diffie–Hellman-type scheme over an insecure channel.

Building on the refuted 2012 permutation-based attack of Kalka–Teichner–Tsaban (KKT), Ben-Zvi, Blackburn, and Tsaban (BBT) present a heuristic attack, published November 13, 2015, that attempts to recover the AEDH shared secret. In their paper BBT reference the AEDH protocol as presented to ISO for certification (ISO 29167-20) by SecureRF. The ISO 29167-20 draft contains two profiles using the Algebraic Eraser. One profile is unaffected by this attack; the second profile is subject to their attack provided the attack runs in real time. This is not the case in most practical deployments.

The BBT attack is simply a targeted attack that does not attempt to break the method, system parameters, or recover any private keys. Rather, its limited focus is to recover the shared secret in a single transaction. In addition, the BBT attack is based on several conjectures that are assumed to hold when parameters are chosen according to standard distributions, which can be mitigated, if not avoided. This paper shows how to choose special distributions so that these conjectures do not hold making the BBT attack ineffective for braid groups with sufficiently many strands. Further, the BBT attack assumes that certain data is available to an attacker, but there are realistic deployment scenarios where this is not the case, making the attack fail completely. In summary, the BBT attack is flawed (with respect to the SecureRF ISO draft) and, at a minimum, over-reaches as to its applicability.

1. Introduction

The Algebraic Eraser Diffie–Hellman protocol (AEDH, originally AEKAP) was introduced in 2005 and published in 2006 by Anshel, Anshel, Goldfeld, and Lemieux [1] as a protocol suitable for use on computationally constrained resource platforms, e.g., FPGAs, ASICs, and wireless sensors. More specifically, AEDH is a Group-Theoretic public-key system designed as a computationally efficient solution for low-power or passive embedded systems and devices associated with, among other things, the Internet of Things (IoT).

In November, 2015, Ben-Zvi, Blackburn, and Tsaban (BBT), leveraging the refuted 2012 permutation-based attack of Kalka, Teichner, and Tsaban (KTT) [3],[1] published a paper [2] claiming a successful attack against AEDH. In the abstract of [2] it is pointed out that certain implementations of AEDH are proposed as an underlying technology for ISO/IEC 29167-20.

Date: January 18, 2016.
1991 *Mathematics Subject Classification.* 20F36, 94A60.
Key words and phrases. Algebraic eraser, colored Burau key agreement protocol, group theoretic cryptography, braid groups.

[1]KKT acknowleged the successful refutation.

The BBT paper presented a heuristic attack that attempts to recover the AEDH shared secret in a single transaction using conjectures assumed to hold when parameters are selected based upon a standard distribution, e.g. a special key choice. These conjectures are only asserted by BBT, they give no indication of how they could be proved.

This paper demonstrates that the BBT attack is flawed (with respect to the SecureRF ISO draft) and, at a minimum, over-reaches as to its applicability. The BBT approach fails to run in real time, fails to take into account that special distributions can be selected to defeat one of its conjectures, and assumes a certain collection of data is available to the attacker, which is not always true.

Specifically, the BBT attack is usually thousands of times slower (on a 4 GHz processor) than the running time of the AEDH protocol in a constrained device with limited computing power and memory. The second profile in the ISO 29167-20 draft is an authentication protocol whereby two users in a lightweight cryptographic setting run the AEDH key agreement protocol and obtain a shared secret which is publicly revealed to complete the authentication. If the BBT attack recovers the shared secret after it is revealed and authentication is completed, it is of no consequence. Thus, the attack fails because the information is no longer relevant.

The BBT attack assumes parameters are chosen according to standard distributions. Practically, the use of a standard distribution in a commercial implementation is an over-simplification; realistic deployment scenarios involve special distributions so that at least one of the BBT conjectures does not hold. As a result, the attack becomes ineffective for braid groups with sufficiently many strands.

The BBT attack assumes that all data required for the attack is available to an attacker. As already published in the referenced ISO specification (29167-20), there exist deployment scenarios in which this assumption is false. Therefore, there are clearly scenarios that are not subject to the BBT attack.

This paper proceeds as follows. In Section 2, we review the AEDH protocol. Next, in Section 3 we summarize the BBT attack, and in Section 4 provide two simple bases for defeating the BBT attack, a conjecture counterexample and deployment counterexample. We conclude in Section 5 by noting that the BBT attack is simply a targeted attack that does not attempt to break the method, system parameters, or recover any private keys.

2. The Algebraic Eraser Diffie–Hellman key agreement protocol.

Let B_N denote the N-strand braid group. Each element in B_N can be expressed as a word in the Artin generators $\{b_1, b_2, \ldots, b_{N-1}\}$, which are subject to the following relations: for $i = 1, \ldots, N-1$, we have

$$b_i b_{i+1} b_i = b_{i+1} b_i b_{i+1}, \tag{1}$$

and for all i, j with $|i - j| \geq 2$, we have

$$b_i b_j = b_j b_i. \tag{2}$$

Thus any $\beta \in B_N$ can be expressed as a product of the form

$$\beta = b_{i_1}^{\epsilon_1} \, b_{i_2}^{\epsilon_2} \, \cdots \, b_{i_k}^{\epsilon_k}, \tag{3}$$

where $i_j \in \{1, \ldots, N-1\}$, and $\epsilon_j \in \{\pm 1\}$.

Each braid $\beta \in B_N$ determines a permutation in S_N, the group of permutations of N letters, as follows. Let $\sigma_i \in S_N$ be the ith simple transposition, which maps $i \mapsto i+1, i+1 \mapsto i$, and leaves $\{1, \ldots, i-1, i+2, \ldots, N\}$ fixed. Then if $\beta \in B_N$ is expressed as in (3), we map β to the permutation $\sigma_\beta = \sigma_{i_1} \cdots \sigma_{i_k}$.

Fix a prime power q, let F_q be the finite field of order q, and let $t_1, \ldots, t_N$ be indeterminates. Consider the group of invertible $N \times N$ matrices with entries in the field of rational functions $F_q(t_1, \ldots, t_N)$, denoted $\mathcal{M}$. Observe the permutation group S_N acts on $\mathcal{M}$ by permuting the variables, and we can hence form the semidirect product $\mathcal{M} \rtimes S_N$. For $i = 1, \ldots, N-1$, let $CB(b_i)$ be the matrix defined by

$$CB(b_i) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & t_i & -t_i & 1 & & \\ & & & \ddots & & \\ & & & & 1 & \end{pmatrix}, \tag{4}$$

where the indicated variables appear in row i, and if $i = 1$ the leftmost t_1 is omitted. We similarly define $CB(b_i^{-1})$ by modifying (4) slightly:

$$CB(b_i^{-1}) = \begin{pmatrix} 1 & & & & & \\ & \ddots & & & & \\ & 1 & -t_{i+1}^{-1} & t_{i+1}^{-1} & & \\ & & & \ddots & & \\ & & & & 1 & \end{pmatrix}.$$

With these matrices in place, each braid generator b_i (respectively, inverse generator b_i^{-1}) determines a Colored Burau/permutation pair $(CB(b_i), \sigma_i)$ (resp., $(CB(b_i^{-1}), \sigma_i)$), and we consider the subgroup of $\mathcal{M} \rtimes S_N$ generated by these colored Burau pairs. Since the pairs $(CB(b_i), \sigma_i)$ satisfy the braid relations (1)–(2), the natural mapping

$$b_i \longmapsto (CB(b_i), \sigma_i)$$

defines a representation $B_N \to \mathcal{M} \rtimes S_N$, called the Colored Burau representation. By fixing a collection of nonzero elements, termed t-values,

$$\{\tau_1, \tau_2, \ldots, \tau_N\} \subset F_q,$$

the mapping $t_i \mapsto \tau_i$ induces a homomorphism

$$\Pi \colon \mathcal{M} \to GL_N(F_q).$$

The operation *e-multiplication* is the right action of the group of colored Burau pairs on the direct product $GL_N(F_q) \times S_N$ and is defined by

$$(m, \sigma_0) \star (CB(\beta), \sigma_\beta) \;=\; (m \cdot \Pi({}^{\sigma_0}\beta), \sigma_0 \sigma_\beta).$$

With these definitions in place, users Alice and Bob execute the AEDH protocol as follows:

System Data:

- A public matrix $m_0 \in GL_N(F_q)$.
- A set of public t-values $\{\tau_1, \tau_2, \ldots, \tau_N\} \subset F_q^\times$.

- Two sets of user conjugates in B_N, one of which is public:

$$\{za_1z^{-1}, za_2z^{-1}, \ldots, za_kz^{-1}\} \quad \text{and} \quad \{zb_1z^{-1}, zb_2z^{-1}, \ldots, zb_\ell z^{-1}\}.$$

  It is assumed that the elements a_i, b_j commute, and that the conjugates are suitably rewritten so that the element $z \in B_N$ remains unknown to the users.

Private/Public Keys:

- Each user chooses a random private matrix m_A, m_B of the form

$$m_A \;=\; \sum f_i m_0^i, \quad m_B \;=\; \sum g_i m_0^i \in F_q[m_0].$$

- Each user chooses a random private braid word w_A, w_B in their respective set of conjugates:

$$\begin{aligned} w_A &\in \langle za_1z^{-1}, za_2z^{-1}, \ldots, za_kz^{-1}\rangle, \\ w_B &\in \langle zb_1z^{-1}, zb_2z^{-1}, \ldots, zb_\ell z^{-1}\rangle. \end{aligned}$$

- The user private keys are given by $(m_A, w_A), (m_B, w_B)$. It is assumed that the user whose conjugates are public will use ephemeral private keys.

- Each user produces and exchanges their respective public keys:

$$\begin{aligned} \mathrm{Pub}_A &= (m_A, 1) \star (CB(w_A), \sigma_{w_A}), \\ \mathrm{Pub}_B &= (m_B, 1) \star (CB(w_B), \sigma_{w_B}). \end{aligned}$$

- Both users evaluate the shared secret K using the received public keys and their private keys:

$$K = (m_A, 1) \cdot Pub_B \star (CB(w_A), \sigma_{w_A}) = (m_B, 1) \cdot Pub_A \star (CB(w_B), \sigma_{w_B}).$$

3. The Ben-Zvi–Blackburn–Tsaban Attack

The BBT attack proceeds as follows. The attacker Eve requires access to the public keys $\mathrm{Pub}_A, \mathrm{Pub}_B$ of Alice and Bob and any other information transmitted over the insecure channel. This includes the t-values $\tau_1, \ldots, \tau_N$, the matrix m_0, and Alice's conjugates $\{za_iz^{-1} \mid i = 1, \ldots, k\}$. Let A be the subgroup of B_N generated by Alice's conjugates. Let C be the subspace $F_q[m_0] \subset M_N(F_q)$ of all polynomials in m_0 over F_q, where $M_N(F_q)$ denotes the vector space of $N \times N$ matrices over F_q.

Let $P \subset A$ be the subgroup of *pure braids* in Alice's subgroup. In particular, P is the kernel of the natural projection $B_N \to S_N$ is restricted to A. The group P determines a subspace $V \subset M_N(F_q)$: we take the subspace spanned by the images $\Pi(w)$ as w ranges over P.

Let $\mathrm{Pub}_A = (p, g)$ be Alice's public key, and let $\mathrm{Pub}_B = (q, h)$ be Bob's public key. To recover the shared secret K, Eve plans to find

- a matrix $\tilde{c} \in C$,

- an element $\alpha' \in V$, and

- an element $(\tilde{a}, g) \;\in\; \langle (CB(\beta), \sigma_\beta) \mid \beta \in B_N \rangle$

satisfying the following property:

$$(p, g) = \tilde{c} \cdot (\alpha', 1) \star (\tilde{a}, g).$$

In other words, Eve seeks a factorization of Alice's public key. Using this data, she then takes pure braids $\alpha_i \in P$ such that the elements $\Pi(\alpha_i)$ give a basis of V, and writes α' as a linear combination

$$\alpha' = \sum_i \lambda_i \Pi(\alpha_i), \quad \lambda_i \in F_q.$$

She then forms the matrix

$$\beta' = \sum_i \lambda_i \Pi({}^h\alpha_i),$$

where the superscript denotes the action of h in the semidirect product. Then BBT prove that the shared secret K can be expressed as

$$K = \tilde{c} \cdot (q\beta', h) \star (\tilde{a}, g).$$

As an example, BBT applied their attack to sample data on the braid group B_{16} and with the finite field F_{256}. The authors successfully recovered the shared secret after a running time of approximately 8 hours and using less than 64 MB of memory.

Eve finds the elements $\tilde{c}$, α', and $\tilde{a}$ needed above to reconstruct K in the following way:

- **Precomputation stage.** Eve first determines a basis of V. Let $\mu_i = (z\alpha_i z^{-1}, g_i)$ be the elements of $\mathcal{M} \rtimes S_N$ corresponding to Alice's conjugates, which are known. Eve requires a method to produce elements g in S_N that have order $r \leq N$ and that are short products of the g_i. BBT assumes this is always possible. Write $g = \prod g(j)^{\varepsilon_j}$, where each $g(j) \in \{g_1, \ldots, g_k\}$ and each $\varepsilon_j \in \{\pm 1\}$, and let $\mu(j)$ be the μ_i corresponding to $g(j)$. Then since g^r is trivial, the product $\alpha = (\prod \mu(j)^{\varepsilon_j})^r$ is pure. Eve constructs many matrices of the form $\Pi(\alpha)$ and stops when she has a set $\alpha_1, \ldots, \alpha_m$ such that the dimension of the span of the $\Pi(\alpha_i)$ has stabilized.

- **Stage 1: Finding $\tilde{a}$.** Let (p, g) be Alice's public key. Eve again must find a product of the μ_i of the form $(\tilde{a}, g)$, that is a product with second component equal to g. This is done using the algorithms in [3].

- **Stage 2: Finding $\tilde{c}$.** Define a matrix γ by $(\gamma, 1) = (p, g) \star (\tilde{a}, g)^{-1}$. The matrix $\tilde{c}$ is then taken to be an invertible element of the intersection $C \cap \gamma V$.

- **Stage 3: Remaining parameters.** The matrix α' is defined to be $\tilde{c}^{-1}\gamma$.

4. Defeating the Ben-Zvi–Blackburn–Tsaban Attack

4.1. Conjecture Counterexample.

As detailed above, in the BBT attack it is assumed that there are many short expressions in the publicly known Reader conjugates which are associated with low order permutations. While this statement holds most of the time, it is not correct in every instance. At the end of their paper, BBT indicate that it may be possible to immunize the Algebraic Eraser against their attack by working with very carefully chosen presentations. The following demonstrates how to effectively produce a set of permutations whose short expressions have high order most of the time, countering their conjecture. The values of the parameter N will necessarily be in

a higher range than is discussed in BBT, but the method can be computationally viable by applying suitable projection operators associated to singular first private matrices.

To counter the conjecture produce a set of $k \geq 2$ permutations

$$\rho_1, \rho_2, \ldots, \rho_k$$

in the symmetric group S_N with the property that almost all short expressions (short words in $\rho_1, \rho_2, \ldots, \rho_k$) have order greater than

$$\alpha_N \cdot e^{\frac{1}{2} \cdot \sqrt{N \log N}},$$

for some constant $\alpha_N > 0$. The constant α_N is yet to be determined, but initial testing shows it is not too small.

Let p_N denote the largest prime such that the sum of the primes less than p_N does not exceed N. By the prime number theorem, we have $p_N \sim \sqrt{N \log N}$.

We then define

$$\begin{aligned}
\rho_1 &:= c_1(3)\, c_1(5)\, c_1(7) \cdots c_1(p_N), \\
\rho_2 &:= c_2(3)\, c_2(5)\, c_2(7) \cdots c_2(p_N), \\
&\vdots \\
\rho_k &:= c_k(3)\, c_k(5)\, c_k(7) \cdots c_k(p_N).
\end{aligned}$$

Here, for every prime p and any $1 \leq i \leq k$, we let $c_i(p)$ denote a p-cycle in S_N. The p-cycles $c_i(p)$ can be randomly chosen and are assumed to satisfy the following additional properties:

- *For each $1 \leq i \leq k$, the cycles $c_i(3), c_i(5), \ldots, c_i(p_N)$ are disjoint.*
- *For each prime $3 \leq p \leq p_n$, the cycles $c_1(p), c_2(p), \ldots, c_k(p)$ all have the same fixed points.*
- *For each prime $3 \leq p \leq p_n$, no two of the cycles $c_1(p), c_2(p), \ldots, c_k(p)$ are integer powers of each other.*

Since the cycles are disjoint, the order of each $\rho_i\, (1 \leq i \leq k)$ is given by the product of primes

$$\prod_{3 \leq p \leq p_N} p \;\sim\; e^{p_N} \;\sim\; \frac{1}{2} \cdot e^{\sqrt{N \log N}},$$

where the above asymptotic formula again follows from the Prime Number Theorem.

To facilitate working with large braid groups one can choose a highly singular seed matrix m_0 in AEDH which has the property that for any $g \in GL_N(F_q)$, the matrix product

$$m_0 \cdot g$$

projects onto a submatrix of g consisting of r rows of g for some small $1 < r < N$. This reduces all the public keys to matrices of size $r \times N$ instead of N^2. In addition, it is possible to work with a much smaller finite field when N is large, and, hence, arrive at manageable public key sizes. It remains to determine optimal parameters for specific applications. This will be the topic of a future paper.

4.2. **Deployment Counterexample.**

The BBT attack requires knowledge of both public keys, the t-values, the seed matrix m_0, and one set of conjugates. Lack of any single one of these items will defeat the attack.

The BBT paper references the ISO 29167-20 draft specification of the Algebraic Eraser. That specification contains two deployment profiles for AEDH. In one of the profiles one party has access to a database that contains public key material for the other parties. Specifically, in this profile an attacker never has access to one of the public keys and, as a result, cannot mount the attack to derive the shared secret. Other deployment scenarios also exist where an attacker does not have access to one or more pieces of data required to mount the attack. In all these scenarios the attack cannot succeed.

5. Conclusions

The BBT attack is simply a targeted attack that does not attempt to break the method, system parameters, or recover any private keys. Its limited focus attempts to recover the shared secret in a single transaction for a class of weak keys. The attack is based on several conjectures, none of which are proven. As per one BBT conjecture, when conjugate material is chosen poorly the attacker can find short expressions and mount an attack. However, when the conjugates are chosen with specific classes of permutations the conjecture fails as does the BBT attack for braid groups with sufficiently many strands. Finding counterexamples of other BBT conjectures is left for a future paper.

Similarly, deployment scenarios (such as one of the profiles in ISO 29167-20) deprive an attacker from the information required to mount the attack. Without all required data the attack cannot even begin.

Therefore, AEDH, a group-theoretic cryptographic protocol that constructs a shared secret via a Diffie–Hellman-type scheme, is secure for many practical applications, including platforms with constrained computation resources, such as FPGAs, ASICs, and wireless sensors.

References

[1] I. Anshel, M. Anshel, D. Goldfeld, and S. Lemieux, *Key agreement, the Algebraic Eraser$^{\text{TM}}$, and lightweight cryptography*, Algebraic methods in cryptography, Contemp. Math., vol. 418, Amer. Math. Soc., Providence, RI, 2006, pp. 1–34.

[2] A. Ben-Zvi, S. Blackburn, and B. Tsaban, *A practical cryptanalysis of the Algebraic Eraser*, preprint, 2015.

[3] A. Kalka, M. Teicher, and B. Tsaban, *Short expressions of permutations as products and cryptanalysis of the Algebraic Eraser*, Adv. in Appl. Math. **49** (2012), no. 1, 57–76.

SecureRF Corporation, 100 Beard Sawmill Rd #350, Shelton, CT 06484
E-mail address: ianshel@securerf.com

SecureRF Corporation, 100 Beard Sawmill Rd #350, Shelton, CT 06484
E-mail address: datkins@securerf.com

SecureRF Corporation, 100 Beard Sawmill Rd #350, Shelton, CT 06484
E-mail address: dgoldfeld@securerf.com

SecureRF Corporation, 100 Beard Sawmill Rd #350, Shelton, CT 06484
E-mail address: pgunnells@securerf.com